The Proof Complexity of Linear Algebra

Michael Soltys and Stephen Cook

August 19, 2003

Abstract

We introduce three formal theories of increasing strength for linear algebra in order to study the complexity of the concepts needed to prove the basic theorems of the subject. We give what is apparently the first feasible proofs of the Cayley-Hamilton theorem and other properties of the determinant, and study the propositional proof complexity of matrix identities such as $AB = I \rightarrow BA = I$.

1 Introduction

The complexity of the basic operations of linear algebra such as the determinant and matrix inverse has been well-studied. Over the field of rationals it lies within the complexity class $\mathbf{NC}^2$, and is complete for the class **DET** [Coo85]. Here we are concerned with the *proof complexity* of linear algebra, which roughly speaking is the complexity of the concepts needed to prove the basic properties of these operations. In general proof complexity has two aspects: uniform and nonuniform (see [Kra95] for a treatise on the subject). The uniform aspect concerns the power of logical theories required to prove a given assertion, while the nonuniform aspect concerns the power of propositional proof systems required to yield polynomial size proofs of a tautology family representing the assertion.

The method of Gaussian elimination can be used to give polynomial time algorithms for the determinant, matrix inverse, etc. (see [Sol02]), but it does not yield the fast parallel algorithms which place these operations in $\mathbf{NC}^2$. We base our treatment of linear algebra on Berkowitz's elegant algorithm [Ber84], which gives field-independent reductions of these operations to matrix powering (the complexity class **DET**) (see [vzG93] for alternative algorithms).

We are interested in the question of whether the basic properties of the determinant can be proved using concepts restricted to the class **DET**, and we make this question precise by defining a quantifier-free theory LAP formalizing reasoning about matrix algebra based on matrix powering. We use LAP to present Berkowitz's algorithm. Since this algorithm computes not only the determinant of a given square matrix A, but also the coefficients of the characteristic polynomial $p_A(x) = \det(xI - A)$, it is natural to ask whether LAP proves the Cayley-Hamilton (C-H) theorem, which asserts $p_A(A) = 0$. We leave this question open, but we demonstrate its importance by showing that LAP proves the equivalence of the C-H theorem with two other basic results: the cofactor expansion of the determinant and the axiomatic definition of the determinant.

If we cannot prove the C-H theorem in LAP, can we at least find a feasible proof; i.e., one using only polynomial time concepts? This question (over finite fields and over the rationals) has a natural precise formalization, since feasible reasoning has been well-studied using $\forall$-equivalent theories such as Cook's PV [Coo75] or Buss's S^1_2 [Bus86]. A study of the linear algebra literature has turned up no such feasible proof, and in fact most proofs of the C-H theorem are based directly or indirectly on the Lagrange expansion of the determinant, which represents an exponential time algorithm.

Thus a major contribution of this paper is our success in finding a feasible proof of the C-H theorem. We formalize this proof in the field-independent theory $\forall$LAP, which extends LAP by allowing induction over formulas with bounded universal matrix quantifiers. We justify the label "feasible" for the proof in several ways, including an interpretation of $\forall$LAP (when the underlying field is finite or the rationals) into the feasible theory V_1^1 (equivalent to Buss's S_2^1). Our feasible proof yields feasible proofs of many basic matrix properties, including the multiplicativity of the determinant, and the correctness of algorithms based on Gaussian elimination.

One specific motivation for this research is to find natural tautology families which may distinguish the power of Frege and Extended Frege (eFrege) propositional proof systems. (A line in a Frege proof is a propositional formula which is an immediate logical consequence of earlier lines, whereas a line in an eFrege proof may also introduce a new propositional variable by definition, allowing for concise abbreviations of exponentially long formulas). The principle

$$AB = I \Longrightarrow BA = I \tag{1}$$

where A and B are $n \times n$ matrices, may provide such an example. This principle (over $\mathbb{Z}_2$ or $\mathbb{Z}$) is readily translated into a tautology INV_n of size polynomial in n. It is plausible to conjecture that the family $\langle \mathrm{INV}_n \rangle$ does not have polynomial size Frege proofs, since the proof of (1) seems to require concepts such as Gaussian elimination or matrix powering whose complexity apparently cannot be expressed by polynomial size propositional formulas (i.e., is not in $\mathbf{NC}^1$). On the other hand, we show that (1) can be proved using polynomial time concepts, and hence (by a general result) $\langle \mathrm{INV}_n \rangle$ does have polynomial size eFrege proofs.

Altogether we introduce three logical theories of increasing power

$$\mathrm{LA} \subset \mathrm{LA}\mathtt{P} \subset \forall \mathrm{LA}\mathtt{P}$$

to formalize linear algebra reasoning. Each theory has three sorts: indices (i.e., natural numbers), field elements, and matrices, and all theorems hold for any choice of the underlying field. The base theory LA allows the basic ring properties of matrices to be formulated and proved. The principle (1) can be formulated in LA but (we conjecture) not proved. We show that LA proves the equivalence of (1) with other "hard" matrix identities. Theorems of LA translate into tautology families with polynomial size Frege proofs.

We extend LA to LAP by adding a new function, $\mathtt{P}$, which is intended to denote matrix powering, i.e., $\mathtt{P}(n, A)$ means A^n. LAP is well suited for formalizing Berkowitz's algorithm, and it is strong enough to prove the equivalence of some fundamental principles of linear algebra. The theorems of LAP translate into quasi-poly-bounded Frege proofs.

We finally extend LAP to $\forall$LAP by allowing induction on formulas with bounded universal matrix quantifiers. This new theory is strong enough to prove the C-H theorem, and hence (by our equivalence) all the major principles of Linear Algebra. The theorems of $\forall$LAP translate into poly-bounded Extended Frege proofs.

This paper is based on the PhD thesis [Sol01] of the first author, which is available on the Web.

2 The Theory LA

We define a quantifier-free theory of Linear Algebra (matrix algebra), and call it LA. Our theory is strong enough to prove the ring properties of matrices such as $A(BC) = (AB)C$ and $A+B = B+A$

but weak enough so that all the theorems of LA (over finite fields or the field of rationals) translate into propositional tautologies with short Frege proofs.

Our theory has three sorts of object: *indices* (i.e., natural numbers), *field elements*, and *matrices*, where the corresponding variables are denoted $i, j, k, \ldots$; $a, b, c, \ldots$; and $A, B, C, \ldots$, respectively. The semantics assumes that objects of type field are from a fixed but arbitrary field, and objects of type matrix have entries from that field.

In fact, almost all results in this paper hold when objects of type field range over an arbitrary commutative ring. Multiplicative inverses are not needed except in the proofs of Lemma 3.1 and Theorem 4.1.

Terms and formulas are built from the following function and predicate symbols, which together comprise the language $\mathcal{L}_{LA}$:

$$\begin{gathered}0_{\text{index}}, 1_{\text{index}}, +_{\text{index}}, *_{\text{index}}, -_{\text{index}}, \mathtt{div}, \mathtt{rem}, \\ 0_{\text{field}}, 1_{\text{field}}, +_{\text{field}}, *_{\text{field}}, -_{\text{field}}, {}^{-1}, \mathtt{r}, \mathtt{c}, \mathtt{e}, \Sigma, \\ \leq_{\text{index}}, =_{\text{index}}, =_{\text{field}}, =_{\text{matrix}}, \text{cond}_{\text{index}}, \text{cond}_{\text{field}}\end{gathered} \tag{2}$$

The intended meanings should be clear, except $-_{\text{index}}$ is cutoff subtraction ($i - j = 0$ if $i < j$), a^{-1} is the inverse of a field element a with $0^{-1} = 0$, and for the following operations on a matrix A: $\mathtt{r}(A), \mathtt{c}(A)$ are the numbers of rows and columns in A, $\mathtt{e}(A, i, j)$ is the field element A_{ij} (where $A_{ij} = 0$ if $i = 0$ or $j = 0$ or $i > \mathtt{r}(A)$ or $j > \mathtt{c}(A)$), $\Sigma(A)$ is the sum of the elements in A. Also $\text{cond}(\alpha, t_1, t_2)$ is interpreted **if** α **then** t_1 **else** t_2, where α is a formula all of whose atomic sub-formulas have the form $m \leq n$ or $m = n$, where m, n are terms of type index, and t_1, t_2 are terms either both of type index or both of type field. (The restriction on α greatly simplifies the propositional translations described in section 6.) The subscripts $_{\text{index}}$, $_{\text{field}}$, and $_{\text{matrix}}$ are usually omitted, since they are clear from the context.

We use n, m for terms of type index, t, u for terms of type field, and T, U for terms of type matrix. Terms of all three types are constructed from variables and the symbols above in the usual way, except that in addition terms of type matrix are either variables $A, B, C, \ldots$ or λ terms $\lambda ij\langle m, n, t\rangle$. Here i and j are variables of type index bound by the λ operator, intended to range over the rows and columns of the matrix. Here also m, n are terms of type index *not* containing i, j (representing the numbers of rows and columns of the matrix) and t is a term of type field (representing the matrix element in position (i, j)).

Atomic formulas have the forms $m \leq n, m = n, t = u, T = U$, where the three occurrences of $=$ should have subscripts $_{\text{index}}$,$_{\text{field}}$,$_{\text{matrix}}$ respectively. Formulas are built from atomic formulas using the propositional connectives $\neg, \vee, \wedge$. Formulas may not have quantifiers.

Note that a precise definition requires terms and formulas to be defined together recursively, because $\text{cond}(\alpha, t_1, t_2)$ is a term whenever α is a formula satisfying the restrictions explained above.

2.1 Defined terms

The λ terms allow us to construct the sum, product, transpose, etc., of matrices. We use the notation $:=$ to introduce abbreviations for terms.

Integer maximum

$$\mathtt{max}\{i, j\} := \text{cond}(i \leq j, j, i)$$

Matrix sum

$$A + B := \lambda ij\langle \mathtt{max}\{\mathtt{r}(A), \mathtt{r}(B)\}, \mathtt{max}\{\mathtt{c}(A), \mathtt{c}(B)\}, A_{ij} + B_{ij}\rangle \tag{3}$$

Note that $A + B$ is well defined even if A and B are incompatible in size, because of our convention that out-of-bound entries are 0.

Scalar product

$$aA := \lambda ij\langle \mathtt{r}(A), \mathtt{c}(A), a * A_{ij}\rangle \tag{4}$$

Matrix transpose

$$A^t := \lambda ij\langle \mathtt{c}(A), \mathtt{r}(A), A_{ji}\rangle \tag{5}$$

Zero and Identity matrices

$$0_{kl} := \lambda ij\langle k, l, 0\rangle \quad \text{and} \quad I_k := \lambda ij\langle k, k, \text{cond}(i = j, 1, 0)\rangle \tag{6}$$

Sometimes we will just write 0 and I when the sizes are clear from the context.

Matrix trace

$$\mathtt{tr}(A) := \Sigma\lambda ij\langle \mathtt{r}(A), 1, A_{ii}\rangle \tag{7}$$

Dot product

$$A \cdot B := \Sigma\lambda ij\langle \mathtt{max}\{\mathtt{r}(A), \mathtt{r}(B)\}, \mathtt{max}\{\mathtt{c}(A), \mathtt{c}(B)\}, A_{ij} * B_{ij}\rangle \tag{8}$$

Matrix product

$$A * B := \lambda ij\langle \mathtt{r}(A), \mathtt{c}(B), \lambda kl\langle \mathtt{c}(A), 1, \mathtt{e}(A, i, k)\rangle \cdot \lambda kl\langle \mathtt{r}(B), 1, \mathtt{e}(B, k, j)\rangle\rangle \tag{9}$$

Finally, the following decomposition of an $n \times n$ matrix A will be used in our axioms defining $\Sigma(S)$ and in presenting Berkowitz's algorithm:

$$A = \begin{pmatrix} a_{11} & R \\ S & M \end{pmatrix} \tag{10}$$

where a_{11} is the $(1,1)$ entry of A, and R, S are $1 \times (n-1)$, $(n-1) \times 1$ submatrices, respectively, and M is the principal submatrix of A Therefore, we make the following precise definitions:

$$\begin{aligned} \mathtt{R}(A) &:= \lambda ij\langle 1, \mathtt{c}(A) - 1, \mathtt{e}(A, 1, i+1)\rangle \\ \mathtt{S}(A) &:= \lambda ij\langle \mathtt{r}(A) - 1, 1, \mathtt{e}(A, i+1, 1)\rangle \\ \mathtt{M}(A) &:= \lambda ij\langle \mathtt{r}(A) - 1, \mathtt{c}(A) - 1, \mathtt{e}(A, i+1, j+1)\rangle \end{aligned} \tag{11}$$

2.2 Proofs in LA

We use Gentzen's sequent calculus LK (with quantifier rules omitted) for the underlying logic (see [Bus98, Chapter 1]). A sequent has the form $\alpha_1, ..., \alpha_k \to \beta_1, ..., \beta_\ell$ where each α_i and β_j is a formula. The intended meaning of the sequent is

$$\forall x_1 \dots x_n \left(\bigwedge_{i=1}^{k} \alpha_i \supset \bigvee_{j=1}^{l} \beta_j \right)$$

where $x_1, \dots, x_n$ is the list of all the free variables of all three sorts that appear in the sequent.

The system LK has the axiom scheme $\alpha \to \alpha$, the structural rules Exchange, Contraction, and Weakening (left and right), the Cut rule, and rules for introducing each of the three connectives $\neg, \vee, \wedge$ on the left and right.

In addition to these axioms and rules, LA has axiom schemes and a rule for equality, an induction rule, and axiom schemes giving the properties of numbers, fields, and matrices.

A *proof* in LA of a sequent S is a finite sequence of sequents ending in S, such that each sequent in the proof is either an axiom, or follows from earlier sequents by a rule of inference. If α is a formula, then we regard a proof of the sequent $\rightarrow \alpha$ as a proof of α.

We now give the axioms of LA (other than the logical axioms $\alpha \rightarrow \alpha$ of LK described above). For each axiom listed below, every legal substitution of terms for free variables is an axiom of LA. Note that in a λ term $\lambda ij\langle m,n,t\rangle$ the variables i,j are bound. Substitution instances must respect the usual rules which prevent free variables from being caught by the binding operator λij. The bound variables i,j may be renamed to any new distinct pair of variables.

Equality Axioms

These are the usual equality axioms, generalized to apply to the three-sorted theory LA. Here $=$ can be any of the three equality symbols, x,y,z are variables of any of the three sorts (as long as the formulas are syntactically correct). In A4, the symbol f can be any of the nonconstant function symbols of LA. However A5 applies only to $\leq$, since this in the only predicate symbol of LA other than $=$.

A1 $\rightarrow x = x$
A2 $x = y \rightarrow y = x$
A3 $(x = y \wedge y = z) \rightarrow x = z$
A4 $x_1 = y_1, ..., x_n = y_n \rightarrow fx_1...x_n = fy_1...y_n$
A5 $i_1 = j_1, i_2 = j_2, i_1 \leq i_2 \rightarrow j_1 \leq j_2$

Axioms for indices

A6 $\rightarrow i + 1 \neq 0$
A7 $\rightarrow i * (j+1) = (i*j) + i$
A8 $i + 1 = j + 1 \rightarrow i = j$
A9 $\rightarrow i \leq i + j$
A10 $\rightarrow i + 0 = i$
A11 $\rightarrow i \leq j, j \leq i$
A12 $\rightarrow i + (j+1) = (i+j) + 1$
A13 $i \leq j, j \leq i \rightarrow i = j$
A14 $\rightarrow i * 0 = 0$
A15 $i \leq j, i + k = j \rightarrow j - i = k$ **and** $i \not\leq j \rightarrow j - i = 0$
A16 $j \neq 0 \rightarrow \mathtt{rem}(i,j) < j$ **and** $j \neq 0 \rightarrow i = j * \mathtt{div}(i,j) + \mathtt{rem}(i,j)$
A17 $\alpha \rightarrow \mathrm{cond}(\alpha, i, j) = i$ **and** $\neg\alpha \rightarrow \mathrm{cond}(\alpha, i, j) = j$

Axioms for field elements

A18 $\rightarrow 0 \neq 1 \wedge a + 0 = a$
A19 $\rightarrow a + (-a) = 0$
A20 $\rightarrow 1 * a = a$
A21[1] $a \neq 0 \rightarrow a * (a^{-1}) = 1$
A22 $\rightarrow a + b = b + a$
A23 $\rightarrow a * b = b * a$
A24 $\rightarrow a + (b+c) = (a+b) + c$
A25 $\rightarrow a * (b*c) = (a*b)*c$
A26 $\rightarrow a * (b+c) = a*b + a*c$
A27 $\alpha \rightarrow \mathrm{cond}(\alpha, a, b) = a$ **and** $\neg\alpha \rightarrow \mathrm{cond}(\alpha, a, b) = b$

[1]This axiom is not used except in the proof of Lemma 3.1 and Theorem 4.1

Axioms for matrices

Axiom A28 states that $\mathtt{e}(A,i,j)$ is zero when i,j are outside the size of A. Axiom A29 defines the behavior of constructed matrices. Axioms A30-A33 define the function Σ recursively by first defining it for row vectors, then column vectors (recall A^t is the transpose of A), and then in general using the decomposition (11). Finally, axiom A34 takes care of empty matrices.

A28 $(i=0 \vee \mathtt{r}(A)<i \vee j=0 \vee \mathtt{c}(A)<j) \to \mathtt{e}(A,i,j)=0$
A29 $\to \mathtt{r}(\lambda ij\langle m,n,t\rangle)=m$ **and** $\to \mathtt{c}(\lambda ij\langle m,n,t\rangle)=n$ **and**
$1\le i, i\le m, 1\le j, j\le n \to \mathtt{e}(\lambda ij\langle m,n,t\rangle,i,j)=t$
A30 $\mathtt{r}(A)=1, \mathtt{c}(A)=1 \to \Sigma(A)=\mathtt{e}(A,1,1)$
A31 $\mathtt{r}(A)=1, 1<\mathtt{c}(A) \to \Sigma(A)=\Sigma(\lambda ij\langle 1,\mathtt{c}(A)-1,A_{ij}\rangle)+A_{1\mathtt{c}(A)}$
A32 $\mathtt{c}(A)=1 \to \Sigma(A)=\Sigma(A^t)$
A33 $1<\mathtt{r}(A), 1<\mathtt{c}(A) \to \Sigma(A)=\mathtt{e}(A,1,1)+\Sigma(\mathtt{R}(A))+\Sigma(\mathtt{S}(A))+\Sigma(\mathtt{M}(A))$
A34 $\mathtt{r}(A)=0 \vee \mathtt{c}(A)=0 \to \Sigma A=0$

Rules for LA

In addition to the logical rules of Gentzen's LK, our system LA has two rules: matrix equality and induction. In specifying the rules below, Γ and Δ are cedents; that is, finite sequences of formulas. We allow either Γ or Δ to be empty.

Matrix equality rule

$$\frac{\Gamma\to\Delta,\mathtt{e}(T,i,j)=\mathtt{e}(U,i,j) \quad \Gamma\to\Delta,\mathtt{r}(T)=\mathtt{r}(U) \quad \Gamma\to\Delta,\mathtt{c}(T)=\mathtt{c}(U)}{\Gamma\to\Delta,T=U}$$

Here the variables i,j may not occur free in the bottom sequent; otherwise T and U are arbitrary matrix terms. Our semantics implies that i and j are implicitly universally quantified in the top sequent. The rule allows us to conclude $T=U$, provided that T and U have the same numbers of rows and columns, and corresponding entries are equal. The rule can be replaced by the axiom $\lambda ij\langle \mathtt{r}(T),\mathtt{c}(T),\mathtt{e}(T,i,j)\rangle = T$ (similar to an η-axiom in lambda calculus) provided that an axiom is also added which is like **A4** with λij replacing f.

Induction rule

$$\frac{\Gamma,\alpha(i)\to\alpha(i+1),\Delta}{\Gamma,\alpha(0)\to\alpha(n),\Delta}$$

Here the variable i (of type index) may not occur free in either Γ or Δ. Also $\alpha(i)$ is any formula, n is any term of type index, and $\alpha(n)$ indicates n is substituted for free occurrences of i in $\alpha(i)$. (Similarly for $\alpha(0)$.)

This completes the description of LA. We finish this section by observing the substitution property in the lemma below. We say that a sequent S' of LA is a *substitution instance* of a sequent S of LA provided that S' results by substituting terms for free variables of S. Of course each term must have the same sort as the variable it replaces, and bound variables must be renamed as appropriate.

Lemma 2.1 Every substitution instance of a theorem of LA is a theorem of LA.

This follows by straightforward induction on LA proofs. The base case follows from the fact that every substitution instance of an LA axiom is an LA axiom.

3 The Theorems of LA

We show that all matrix identities which state that the set of $n \times n$ matrices form a ring, and all identities that state that the set of $m \times n$ matrices form a module over the underlying field, are theorems of LA. However, LA is apparently not strong enough to prove matrix identities which require arguing about inverses. We present four such examples at the end of this section, and show that LA proves their equivalence.

Formally an LA proof of an identity $T = U$ is a sequent derivation of $\rightarrow T = U$ from the axioms and rules presented in the previous section. Below we present at most informal sketches of these formal proofs.

In general, we use the following strategy to prove a matrix identity $T = U$. We first show that $\mathtt{r}(T) = \mathtt{r}(U)$ and $\mathtt{c}(T) = \mathtt{c}(U)$, and then we show $\mathtt{e}(T,i,j) = \mathtt{e}(U,i,j)$, from which we can conclude that $T = U$ by the matrix equality rule. Thus we conclude two matrices are equal if they have the same size and same entries.

For the sake of readability we will omit "$*$" (the multiplication symbol), as it will always be clear from the context when it is required.

Refer to section 2.1 for definitions of terms such as $\mathtt{max}\{i,j\}$ and $A + 0_{kl}$.

The results in the section (except the Odd Town Theorem at the end) continue to hold when the underlying field is replaced by any commutative ring.

Ring properties

T1 $A + 0_{\mathtt{r}(A)\mathtt{c}(A)} = A$

Proof. The row and column identities follows from $\mathtt{max}\{i,i\} = i$. Equality of corresponding entries follows from the the field axiom A18 stating $a + 0 = a$. □

T2 $A + (-1)A = 0_{\mathtt{r}(A)\mathtt{c}(A)}$

Proof. Equality of corresponding entries follows from the field property $a + (-1)a = 0$. □

Commutativity and associativity of matrix addition follow from the corresponding field properties, together with theorems T3 and T5 below to derive the row and column identities.

T3 $\mathtt{max}\{i,j\} = \mathtt{max}\{j,i\}$

T4 $A + B = B + A$

T5 $\mathtt{max}\{i,\mathtt{max}\{j,k\}\} = \mathtt{max}\{\mathtt{max}\{i,j\},k\}$

T6 $A + (B + C) = (A + B) + C$

Before we prove the next theorem, we outline a strategy for proving claims about matrices by induction on their size. The first thing to note is that it is possible to define empty matrices (matrices with zero rows or zero columns), but we consider such matrices to be special. Our theorems hold for this special case, by axioms A28 and A34, so we will always implicitly assume that it holds. Thus, the Basis Case in the inductive proofs that will follow, is when there is one row (or one column). Therefore when applying the Induction rule, instead of doing induction on i we do induction on j, where $i = j + 1$.

Also note that the size of a matrix has two parameters: the number of rows, and the number of columns. We deal with this problem as follows: suppose that we want to prove something for all matrices A. We define a new (constructed) matrix $M(i, A)$ as follows: first let $d(A)$ be:

$$d(A) := \text{cond}(\mathtt{r}(A) \leq \mathtt{c}(A), \mathtt{r}(A), \mathtt{c}(A))$$

that is, $d(A) = \min\{\mathtt{r}(A), \mathtt{c}(A)\}$. Now let:

$$M(i, A) := \lambda pq\langle \mathtt{r}(A) - d(A) + i, \mathtt{c}(A) - d(A) + i, \mathtt{e}(A, d(A) - i + p, d(A) - i + q)\rangle$$

that is, $M(i, A)$ is the i-th principal submatrix of A. To prove that a property $\mathcal{P}$ holds for A, we prove that $\mathcal{P}$ holds for $M(1, A)$ (Basis Case), and we prove that if $\mathcal{P}$ holds for $M(i, A)$, it also holds for $M(i + 1, A)$ (Induction Step). From this we conclude, by the Induction rule, that $\mathcal{P}$ holds for $M(d(A), A)$, and $M(d(A), A)$ is just A. Note that in the Basis Case we might have to prove that $\mathcal{P}$ holds for a row vector or a column vector, which is a $k \times 1$ or a $1 \times k$ matrix, and this in turn can also be done by induction (on k).

T7 $\Sigma 0_{kl} = 0_{\text{field}}$

Proof. This follows by induction as outlined above, using the axioms A30-A33 giving a recursive definition of Σ. □

T8 $AI_{\mathtt{c}(A)} = A$ and $I_{\mathtt{r}(A)}A = A$

Proof. For the first case, equality of entries is proved by induction on $c(A)$, using T7 when entries are out of bounds. □

The next four theorems are helpful for proving the associativity of matrix multiplication, T13.

T9 $\Sigma(cA) = c\Sigma(A)$

T10 $\Sigma(A + B) = \Sigma(A) + \Sigma(B)$

The next theorem states that we can "fold" a matrix into a column vector. That is, if we take Σ of each row, then the Σ of the resulting column vector is the same as the Σ of the original matrix.

T11 $\Sigma A = \Sigma\lambda ij\langle \mathtt{r}(A), 1, \Sigma\lambda kl\langle 1, \mathtt{c}(A), A_{il}\rangle\rangle$

Proof. Induction on $r(A)$, using A30-A33. □

T12 $\Sigma(A) = \Sigma(A^t)$

Proof. Induction on $r(A)$, using A30-A33 and the definition of A transpose (section 2.1). □

T13 $A(BC) = (AB)C$

Proof. The idea is to show that the sum of all entries in a matrix can be computed either by summing along the rows first, or by summing along the columns first. This can be formalized using T9-T12. No induction is needed. □

T14 $\texttt{max}\{i, \texttt{max}\{j,k\}\} = \texttt{max}\{\texttt{max}\{i,j\}, \texttt{max}\{i,k\}\}$

T15 $A(B+C) = AB + AC$

Proof. The row and column identities are proved using the properties of `max`, including T14. The equality of corresponding entries follows from the distributive law for fields (A26), together with T10. □

T16 $(B+C)A = BA + CA$

Module properties

T17 $(a+b)A = aA + bA$

T18 $a(A+B) = aA + aB$

T19 $(ab)A = a(bB)$

Inner product

The following theorems show that our dot product is in fact an inner product:

T20 $A \cdot B = B \cdot A$

T21 $A \cdot (B+C) = A \cdot B + A \cdot C$

T22 $aA \cdot B = a(A \cdot B)$

Miscellaneous theorems

T23 $a(AB) = (aA)B \wedge (aA)B = A(aB)$

T24 $(AB)^t = B^t A^t$

T25 $I_k^t = I_k \wedge 0_{kl}^t = 0_{lk}$

T26 $(A^t)^t = A$

3.1 Hard matrix identities

In this section we present four matrix identities which we call *hard matrix identities*. They are hard in the sense that they seem to require computing inverses in their derivations, and therefore appear not to be provable in the theory LA. We show however that LA proves that each is equivalent to each of the others.

$$AB = I, AC = I \rightarrow B = C \qquad \text{I}$$
$$AB = I \rightarrow AC \neq 0, C = 0 \qquad \text{II}$$
$$AB = I \rightarrow BA = I \qquad \text{III}$$
$$AB = I \rightarrow A^t B^t = I \qquad \text{IV}$$

Identity III was proposed by the second author as a candidate for the separation of Frege and Extended Frege propositional proof systems. The relation between theorems of LA and the power of propositional proof systems is discussed in section 6.

Theorem 3.1 LA proves the equivalence I $\Leftrightarrow$ II $\Leftrightarrow$ III $\Leftrightarrow$ IV.

Proof. We show that I $\Rightarrow$ II $\Rightarrow$ III $\Rightarrow$ IV $\Rightarrow$ I.
I $\Rightarrow$ II Assume $AB = I \wedge AC = 0$. By A4, $AB + AC = I + 0$, and by T1 and T15, $A(B+C) = I$. Using I, $B = B + C$, so by T2, $C = 0$.
II $\Rightarrow$ III Assume $AB = I$. By A1 and A4, $(AB)A = IA$, by T2, $(AB)A + (-1)IA = 0$, by T13 and T23, $A(BA) + A(-1)I = 0$, and by T15, $A(BA + (-1)I) = 0$. By II, $BA + (-1)I = 0$, and by T2, $BA = I$.
III $\Rightarrow$ IV Assume $AB = I$. By III, $BA = I$, and by A29 $(BA)^t = I^t$. By T24, we obtain $A^tB^t = I$.
IV $\Rightarrow$ I Assume $AB = I \wedge AC = I$. By T2 $AB + (-1)AC = 0$, by T23, $AB + A(-1)C = 0$, by T15, $A(B + (-1)C) = 0$, by T13, $(BA)(B + (-1)C) = 0$. Now, using transpose property T24, we get $(B + (-1)C)^t(BA)^t = 0$, and since $AB = I$, by IV, $A^tB^t = I$, so by T24 again, $(BA)^t = I$, so we obtain that $(B + (-1)C)^t = 0$, so $B + (-1)C = 0$, so $B = C$. □

There is one more identity equivalent to I–IV, proposed by C. Rackoff:

$$\text{If } A, B \text{ are } n \times n \text{ and the last column of } A \text{ is } 0, \text{ then } AB \neq I \tag{V}$$

Lemma 3.1 LA proves (using the field inverse axiom **A21**) the equivalence of V and I–IV.

Proof. It is easy to see that III implies V. To show that V implies II, we prove the contrapositive. Suppose that II is false, so that $AB = I, AC = 0$, and $C \neq 0$. Then for some column vector $X \neq 0$ we have that $AX = 0$. It follows that the columns of A must be linearly dependent. Let A_i denote the i-th column of A. Using the field inverse axiom **A21** we may suppose that $A_n = c_1A_1 + c_2A_2 + \cdots + c_{n-1}A_{n-1}$ (if this is not the case for the n-th column it will be true for some column A_i, and we can place A_i at the end of the matrix using a permutation matrix).

Let A' be A with the last column, A_n, replaced by a column of zeros. Let B' be B, with the following modification: the i-th row of B', for $1 \leq i < n$, is the sum of the i-th row of B with the last row of B multiplied by c_i, and the last row of B' is zero (or anything, it does not really matter).

Then, $A'B' = I$, because $AB = I$. But the last column of A' is zero, which contradicts V. □

The Odd Town Theorem was proposed in [BBP94] as an example generating tautologies hard for Frege systems. This theorem states the following: Suppose a town has n citizens, and that there is a set of clubs, each consisting of citizens, such that each club has an odd number of members, and such that every two clubs have an even number of members in common. Then there are no more than n clubs.

It is not hard to see that LA, together with the axiom $a = 0 \vee a = 1$ (asserting that the underlying field is $\mathbb{Z}_2$), proves the Odd Town Theorem from the assumption III above. Suppose that the town satisfies the hypotheses of the theorem, and the town has n citizens and m clubs, where $m > n$. Let A be a $m \times m$ matrix in which A_{ij} is 1 if citizen i is in club j, and 0 otherwise. Then the last $m - n$ columns of A are 0. By the hypotheses concerning clubs, it follows that $AA^t = I_m$. Therefore, by III, $A^tA = I_m$. But this is impossible, since the top row of A^t is 0.

It is an open question whether LA (over any field) proves the hard identities, or the Odd Town Theorem.

4 Berkowitz's Algorithm and LAP

Berkowitz's algorithm allows us to reduce the computation of the characteristic polynomial of an $n \times n$ matrix A, traditionally given by $p_A(x) = \det(xI - A)$, to the operation of matrix powering.

This algorithm, and all results in this section except Theorem 4.1, continue to hold when the underlying field is replaced by any commutative ring.

We begin by presenting an extension LAP to the system LA which includes matrix powering.

4.1 The theory LAP

We add a new binary function symbol P to the language $\mathcal{L}_{LA}$ of LA to form the language $\mathcal{L}_{\mathrm{LAP}}$ of the theory LAP. (Here $\mathtt{P}(n, A)$ is intended to mean A^n.) The axiom schemes and rules of LAP are the same as for LA, except for two additional axiom schemes which give a recursive definition of P:

A35 $\rightarrow \mathtt{P}(0, A) = I$
A36 $\rightarrow \mathtt{P}(n+1, A) = \mathtt{P}(n, A) * A$.

As in the case of the other axiom schemes, n can be replaced by any $\mathcal{L}_{\mathrm{LAP}}$ term of type index and A can be replaced by any $\mathcal{L}_{\mathrm{LAP}}$ term of type matrix.

We can express iterated matrix product in LAP using the standard method of reducing this to matrix powering. Let $A_1, A_2, \ldots, A_m$, be a sequence of square matrices of equal size. To compute the iterated matrix product $A_1 A_2 \cdots A_m$, we place these matrices into a single big matrix C, above the main diagonal of C. More precisely, assume that the A_i's are $n \times n$ matrices. Then, C is a $(m+1)n \times (m+1)n$ matrix of the form:

$$\begin{pmatrix} 0 & A_1 & 0 & \cdots & 0 \\ 0 & 0 & A_2 & \cdots & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & \cdots & A_m \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Now, compute C^m. The product $A_1 A_2 \ldots A_m$ is the $n \times n$ upper-right corner of C^m.

4.2 Berkowitz's algorithm

Suppose we decompose the $n \times n$ matrix A according to (10). That is,

$$A = \begin{pmatrix} a_{11} & R \\ S & M \end{pmatrix} \tag{12}$$

where R is an $1 \times (n-1)$ row matrix and S is a $(n-1) \times 1$ column matrix and M is $(n-1) \times (n-1)$. Let $p(x)$ and $q(x)$ be the characteristic polynomials of A and M respectively. Suppose that the coefficients of p form the column vector

$$p = \begin{pmatrix} p_n & p_{n-1} & \ldots & p_0 \end{pmatrix}^t \tag{13}$$

where p_i is the coefficient of x^i in $\det(xI - A)$, and similarly for q. Then Berkowitz [Ber84] showed

$$p = C_1 q \tag{14}$$

where C_1 is an $(n+1) \times n$ Toeplitz lower triangular matrix (Toeplitz means that the values on each diagonal are the same) and where the entries in the first column are defined as follows:

$$c_{i1} = \begin{cases} 1 & \text{if } i = 1 \\ -a_{11} & \text{if } i = 2 \\ -(RM^{i-3}S) & \text{if } i \geq 3 \end{cases} \tag{15}$$

For example, If A is a 4×4 matrix, then $p = C_1 q$ is given by:

$$\begin{pmatrix} p_4 \\ p_3 \\ p_2 \\ p_1 \\ p_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -a_{11} & 1 & 0 & 0 \\ -RS & -a_{11} & 1 & 0 \\ -RMS & -RS & -a_{11} & 1 \\ -RM^2S & -RMS & -RS & -a_{11} \end{pmatrix} \begin{pmatrix} q_3 \\ q_2 \\ q_1 \\ q_0 \end{pmatrix} \tag{16}$$

Berkowitz's algorithm consists in repeating this for q, and continuing so that p is expressed as a product of matrices:

$$p = C_1 C_2 \cdots C_n \tag{17}$$

where C_i is an $(n+2-i) \times (n+1-i)$ Toeplitz matrix defined as in (15) except A is replaced by its i-th principal sub-matrix.

4.3 Defined terms and theorems in LAP

The right-hand side of (17) can be expressed as a term in LAP using the method given by (16). We use this term as the definition in LAP of the characteristic polynomial p, given in (13), of the matrix A. (If $n = 1$ and $A = (a)$, then $p = (1 \quad -a)^t$.)

Also in LAP we define

$$\det(A) := (-1)^n p_0 \tag{18}$$

where p_0 is as in (13), and we define

$$\operatorname{adj}(A) := (-1)^{n-1}(p_n A^{n-1} + p_{n-1} A^{n-2} + \ldots + p_1 I) \tag{19}$$

Recall that in the usual definition, the (i,j)-th entry of the adjoint of A is $(-1)^{i+j}\det(A[i|j])$, where $A[i|j]$ is the minor obtained by deleting the i-th row and j-th column of A. The equivalence of this and (19) can be proved in LAP using the Cayley-Hamilton (C-H) Theorem as an assumption.

Recall that the C-H theorem states that $p(A) = 0$. From (19) we have that:

$$A \operatorname{adj}(A) = (-1)^{n-1}(p(A) - p_0 I)$$

Assuming $p(A) = 0$ we have by (18) that:

$$A \operatorname{adj}(A) = \operatorname{adj}(A) A = \det(A) I \tag{20}$$

In fact LAP easily proves the equivalence of (20) with the C-H theorem. We also have

Theorem 4.1 LAP (over any field) proves that the C-H theorem implies the hard matrix identities I–IV of section 3.

Proof. It suffices to consider the identity III:

$$AB = I \to BA = I$$

Using the assumption $AB = I$ it suffices to show that there is *some* left inverse C of A, since using simple ring properties of matrices (formalizable in LA) it is easy to show $AB = I$ and $CA = I$ implies $BA = I$.

To show that a left inverse C exists, we use the C-H theorem $p(A) = 0$, where p is the characteristic polynomial of A. Since p is not the zero polynomial (it has leading coefficient 1), there must be $k \geq 0$ and a polynomial q such that

$$0 = p(A) = q(A)A^k \tag{21}$$

where q has a nonzero constant term. From $AB = I$ we can show in LAP by induction on i that $A^i B^i = I$. Thus multiplying (21) on the right by B^k we obtain $q(A) = 0$, which we can write as

$$\hat{q}(A)A = -q_0 I$$

where q_0 is the constant coefficient of q. Dividing by $-q_0$ we obtain the required left inverse $C = (-1/q_0)\hat{q}(A)$. □

It is an open question whether LAP proves the C-H theorem in general, although it does prove the C-H theorem for triangular matrices [Sol01].

By the *axiomatic definition of the determinant* we mean that the determinant function $\det(A)$ satisfies the three conditions

- det is multi-linear in the rows and columns of A
- det is alternating in the rows and columns of A
- if $A = I$, then $\det(A) = 1$

It is well-known that these conditions completely characterize the determinant.

By the *cofactor expansion* we mean for every $1 \leq i \leq n$

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A[i|j]) \tag{22}$$

where $A[i|j]$ denotes the matrix obtained from A by removing the i-th row and the j-th column. For each i, the RHS of the equation is called the *cofactor expansion of A along the i-th row*, and (22) states that we obtain $\det(A)$ expanding along any row of A. Applying this recursively results in an exponential time algorithm for computing $\det(A)$, showing that the expansion completely defines the determinant.

By the *multiplicativity of the determinant* we mean

$$\det(AB) = \det(A)\det(B)$$

where A, B are $n \times n$ matrices.

The following is the major result of this section.

Theorem 4.2 LAP (over any commutative ring) proves the equivalence of the following principles:

1. C-H theorem
2. Axiomatic definition of det
3. Cofactor Expansion

and LAP also proves the following implications:

4. Multiplicativity of det $\Longrightarrow$ C-H theorem
5. C-H Theorem + $\{\det(A) = 0 \rightarrow AB \neq I\}$ $\Longrightarrow$ Multiplicativity of det.

The rest of section 4 will consist of the proof of this theorem. The proof is long, so it is given in four sections: 4.4 ($1 \Longrightarrow 2$), 4.5 ($2 \Longrightarrow 3$), 4.6 ($3 \Longrightarrow 1$), and 4.7 (implications 4 and 5).

In section 5, we will show that the multiplicativity of the determinant can be proven in the theory $\forall$LAP, which is an extension of LAP where we allow induction on formulas with a bounded universal matrix quantifier (i.e., formulas of the form $\forall X \leq n\alpha$, where α has no quantifiers, and X is a variable of type matrix, with $\mathtt{r}(X) \leq n$ and $\mathtt{c}(X) \leq n$). From this, and from 4 above, it follows that all the principles listed above can be proven in $\forall$LAP. Since we show that all the theorems of $\forall$LAP have feasible proofs, it will follow that all these principles have feasible proofs.

The following lemmas are needed in the proof of Theorem 4.2.

Lemma 4.1 LAP proves
$$\det(A) = a_{11}\det(M) - R\ \mathrm{adj}(M)\ S \tag{23}$$
where A is given by (12).

Proof. Using the definition of det (given by (18)) we have:
$$\det(A) = (-1)^n (p_A)_0$$
where $(p_A)_0$ denotes the constant coefficient of the characteristic polynomial of A. From Berkowitz's algorithm and the definition of the adjoint (given by (19)):
$$= (-1)^n(-a_{11}(p_M)_0 - (-1)^{n-2} R\ \mathrm{adj}(M)\ S)$$
since LAP proves $(-1)^{\text{even power}} = 1$, we have:
$$= a_{11}(-1)^{n-1}(p_M)_0 - R\ \mathrm{adj}(M)\ S$$
and by using (18) one more time:
$$= a_{11}\det(M) - R\ \mathrm{adj}(M)\ S$$
This argument can be clearly formalized in LAP. $\square$

Lemma 4.2 LAP proves that A and A^t have the same characteristic polynomial, i.e., $p_A = p_{A^t}$.

Proof. The proof is by induction on the size of A. The Basis Case is trivial because $(a)^t = (a)$. Suppose now that A is an $n \times n$ matrix, $n > 1$. By the IH we know that $p_M = p_{M^t}$. Furthermore, if we consider the matrix C_1 in the definition of Berkowitz's algorithm, we see that the entries 1 and $-a_{11}$ do not change under transposition of A, and also, since $S(M^t)^k R$ is a 1×1 matrix, it follows that $S(M^t)^k R = (S(M^t)^k)R)^t = RM^k S$, so in fact C_1 is the same for A and A^t. This gives us the result. $\square$

4.4 The axiomatic definition of determinant

We show that when the determinant is defined as in (18), the axiomatic definition of the determinant follows from the C-H theorem, and that this can be proven in LAP. The condition $\det(I) = 1$ is easy, and multilinearity in the first row (and column) is easy as well. Thus, the whole proof hinges on an LAP proof of alternation from the C-H theorem.

It is in fact enough to prove alternation in the rows, as alternation in the columns will follow from alternation in the rows by $\det(A) = \det(A^t)$ (Lemma 4.2).

Definition 4.1 I_{ij} is the matrix obtained from the identity matrix by interchanging the i-th and j-th rows. I_i is the same as $I_{i,i+1}$.

The effect of multiplying A on the left by I_{ij} is that of interchanging the i-th and j-th rows of A. On the other hand, AI_{ij} is A with the i-th and j-th columns interchanged.

We show alternation in the rows by first showing that for any matrix A, A and I_1AI_1 have the same characteristic polynomial ($I_1 = I_{1,2}$, so I_1AI_1 is the matrix A with the first two rows interchanged, and the first two columns interchanged). This is done in Lemma 4.3.

Then, we show that A and I_iAI_i have the same characteristic polynomial for any i ($I_i = I_{i,i+1}$). This is done Lemma 4.5.

Finally, we obtain that A and $I_{ij}AI_{ij}$ have the same char poly (as any permutation is a product of transpositions).

We also show that $\det(A) = -\det(I_1A)$. From this it follows that $\det(A) = -\det(I_{1i}A)$ for all i, since we can bring the i-th row to the second position (via $I_{2i}AI_{2i}$), and reorder things (by applying $I_{2i}AI_{2i}$ once more). Since $I_{ij} = I_{1i}I_{1j}I_{1i}$, this gives us alternation in the rows.

Note that we prove that A and $I_{ij}AI_{ij}$ have the same char poly, i.e., $p_{I_{ij}AI_{ij}} = p_A$, to be able to reorder the matrix and prove alternation.

Lemma 4.3 Let A be an $n\times n$ matrix, and let $M_2 = (A[1|1])[1|1]$ be the second principal submatrix of A. Then, LAP proves the following implication: $p_{M_2}(M_2) = 0 \Longrightarrow p_{(I_1AI_1)} = p_A$. That is, LAP proves that if the C-H Theorem holds for M_2, then I_1AI_1 and A have the same characteristic polynomial.

Proof. Let A be of the following form:

$$A = \begin{pmatrix} a & b & R \\ c & d & P \\ S & Q & M_2 \end{pmatrix}$$

where M_2 is an $(n-2)\times(n-2)$ matrix, a, b, c, d are entries, and R, P, S^t, Q^t are $1\times(n-2)$ matrices. We define σ to be the permutation that exchanges the first two rows, and the first two columns of A. Formally:

$$\begin{gathered} a,b,c,d \overset{\sigma}{\mapsto} d,c,b,a \\ R,S,P,Q \overset{\sigma}{\mapsto} P,Q,R,S \\ M_2 \overset{\sigma}{\mapsto} M_2 \end{gathered}$$

For the sake of readability, we let $M = M_2$.

Recall that $p_A = C_1C_2C_3\cdots C_n$. To show that $p_A = p_{I_1AI_1}$, we first show that all the entries of C_1C_2, *except* for those in the last row, remain invariant under σ. Since $C_3\cdots C_n$ are not affected by σ, this will give us that, *except* for the last row, $p_A = p_{I_1AI_1}$. Then, we show that the last entries are also invariant under σ, that is, $(p_A)_0 = (p_{I_1AI_1})_0$, but for this we do need the C-H Theorem.

We start by showing that all the entries of C_1C_2, except for those in the last row, are invariant under σ. Note that we do not need the C-H Theorem for this.

Let $C[i|j]$ denote the matrix C with row i and column j removed. Let $C[i|-]$ and $C[-|j]$ denote the matrix C with row i removed (and no columns removed) and column j removed (and no rows removed), respectively.

Note that $(C_1C_2)[n+1|-]$ is a lower-triangular Toeplitz matrix. We consider the first column of $(C_1C_2)[n+1|-]$. The top three entries of the first column are:

$$\begin{gathered} 1 \\ -a-d \\ -\begin{pmatrix} b & R \end{pmatrix}\begin{pmatrix} c \\ S \end{pmatrix} + ad - PQ = -bc - RS + ad - PQ \end{gathered}$$

By inspection, they are all invariant under σ.

The $(k+1)$-st entry in the first column, for $k \geq 3$, is given by taking the dot-product of the following two vectors:

$$\begin{pmatrix} 1 \\ -a \\ -\begin{pmatrix} b & R \end{pmatrix}\begin{pmatrix} c \\ S \end{pmatrix} \\ -\begin{pmatrix} b & R \end{pmatrix}\begin{pmatrix} d & P \\ Q & M \end{pmatrix}\begin{pmatrix} c \\ S \end{pmatrix} \\ \vdots \\ -\begin{pmatrix} b & R \end{pmatrix}\begin{pmatrix} d & P \\ Q & M \end{pmatrix}^{k-2}\begin{pmatrix} c \\ S \end{pmatrix} \end{pmatrix}, \quad \begin{pmatrix} -PM^{k-2}Q \\ -PM^{k-3}Q \\ \vdots \\ -PQ \\ -d \\ 1 \end{pmatrix} \tag{24}$$

We are going to prove that this dot-product is invariant under σ. This dot-product can be expressed as follows:

$$\begin{pmatrix} b & R \end{pmatrix}\begin{pmatrix} w_k & X_k \\ Y_k & Z_k \end{pmatrix}\begin{pmatrix} c \\ S \end{pmatrix} + aPM^{k-3}Q - PM^{k-2}Q \tag{25}$$

where:

$$\begin{pmatrix} w_k & X_k \\ Y_k & Z_k \end{pmatrix} = -\begin{pmatrix} d & P \\ Q & M \end{pmatrix}^{k-2} + d\begin{pmatrix} d & P \\ Q & M \end{pmatrix}^{k-3} + \sum_{i=0}^{k-4} PM^{k-4-i}Q\begin{pmatrix} d & P \\ Q & M \end{pmatrix}^{i} \tag{26}$$

We first show by induction on $k \geq 3$ that the following holds:

$$\begin{cases} w_k = 0 \\ X_k = -PM^{k-3} \\ Y_k = -M^{k-3}Q \\ Z_k = -M^{k-2} + dM^{k-3} + \sum_{i=0}^{k-4}((PM^{k-4-i}Q)M^i - M^iQPM^{k-4-i}) \end{cases} \tag{27}$$

The basis case is $k = 3$:

$$\begin{pmatrix} w_3 & X_3 \\ Y_3 & Z_3 \end{pmatrix} = -\begin{pmatrix} d & P \\ Q & M \end{pmatrix} + dI$$

and indeed it holds. Now, to prove the induction step, assume that the result holds for k, and show that it also holds for $k+1$ (notice that clearly the induction step can be formalized in LAP). Using (26) we have:

$$\begin{pmatrix} w_{k+1} & X_{k+1} \\ Y_{k+1} & Z_{k+1} \end{pmatrix} = \begin{pmatrix} d & P \\ Q & M \end{pmatrix}\begin{pmatrix} w_k & X_k \\ Y_k & Z_k \end{pmatrix} + (PM^{k-3}Q)I \tag{28}$$

Now, using the induction hypothesis (and note that the induction hypothesis is *all four properties*):

1. Show that $w_{k+1} = 0$.

$$w_{k+1} = dw_k + PY_k + (PM^{k-3}Q) = d \cdot 0 + P(-M^{k-3}Q) + (PM^{k-3}Q) = 0$$

2. Show that $X_{k+1} = -PM^{k-2}$.

$$\begin{aligned} X_{k+1} &= dX_k + PZ_k \\ &= d(-PM^{k-3}) + P\left(-M^{k-2} + dM^{k-3} + \sum_{i=0}^{k-4}((PM^{k-4-i}Q)M^i - M^iQPM^{k-4-i})\right) \\ &= -PM^{k-2} \end{aligned}$$

since $P(PM^{k-2-i}Q)M^i = (PM^{k-2-i}Q)PM^i$.

3. Show that $Y_{k+1} = -M^{k-2}Q$.

$$Y_{k+1} = w_kQ + MY_k = 0 \cdot Q + M(-M^{k-3}Q) = -M^{k-2}Q$$

4. Show that $Z_{k+1} = -M^{k-1} + dM^{k-2} + \sum_{i=0}^{k-3}((PM^{k-3-i}Q)M^i - M^iQPM^{k-3-i})$.

$$\begin{aligned} Z_{k+1} &= QX_k + MZ_k + (PM^{k-3}Q)I \\ &= Q(-PM^{k-3}) + M\left(-M^{k-2} + dM^{k-3} + \sum_{i=0}^{k-4}((PM^{k-4-i}Q)M^i - M^iQPM^{k-4-i})\right) \\ &\quad + (PM^{k-3}Q)I \end{aligned}$$

and grouping all the terms we get:

$$= -M^{k-1} + dM^{k-2} + \sum_{i=0}^{k-3}((PM^{k-3-i}Q)M^i - M^iQPM^{k-3-i})$$

We show in some detail this last step:

$$\begin{aligned} &M\sum_{i=0}^{k-4}(PM^{k-4-i}Q)M^i - M^iQPM^{k-4-i} = \sum_{i=0}^{k-4}(PM^{k-4-i}Q)M^{i+1} - M^{i+1}QPM^{k-4-i} \\ &= \sum_{i=0}^{k-4}(PM^{k-3-(i+1)}QM^{i+1} - M^{i+1}QPM^{k-3-(i+1)} = \sum_{i=1}^{k-3}(PM^{k-3-i}Q)M^i - M^iQPM^{k-3-i} \\ &= -PM^{k-3}Q + QPM^{k-3} + \sum_{i=0}^{k-3}(PM^{k-3-i}Q)M^i - M^iQPM^{k-3-i} \end{aligned}$$

This ends the proof of the induction step, and the proof of (27).

Using (27) we can prove that:

$$\begin{pmatrix} b & R \end{pmatrix}\begin{pmatrix} w_k & X_k \\ Y_k & Z_k \end{pmatrix}\begin{pmatrix} c \\ S \end{pmatrix} + aPM^{k-3}Q - PM^{k-2}Q \tag{29}$$

is invariant under σ. We expand and obtain:

$$\begin{aligned} &-bPM^{k-2}S - cRM^{k-2}Q - RM^{k-2}S + dRM^{k-3}S \\ &+\sum_{i=0}^{k-4} R((PM^{k-4-i}Q)M^i - M^iQPM^{k-4-i})S + aPM^{k-3}Q - PM^{k-2}Q \end{aligned} \tag{30}$$

Now note that the following pairs of terms are invariant under σ:

$$\{-bPM^{k-2}S, -cRM^{k-2}Q\} \qquad \{-RM^{k-2}S, -PM^{k-2}Q\} \qquad \{+dRM^{k-3}S, +aPM^{k-3}Q\}$$

Therefore, to show that (29) is invariant under σ, it remains to show that the summation is invariant under σ, and the summation is equal to:

$$\sum_{i=0}^{k-4}(PM^{k-4-i}Q)(RM^iS) - \sum_{i=0}^{k-4}(RM^iQ)(PM^{k-4-i}S)$$

Note that:

$$(PM^{k-4-i}Q)(RM^iS) \xmapsto{\sigma} (RM^{k-4-i}S)(PM^iQ)$$
$$(RM^iQ)(PM^{k-4-i}S) \xmapsto{\sigma} (PM^iS)(RM^{k-4-i}Q)$$

So clearly each of the two summations is "closed" under σ, and hence invariant.

To finish the proof of Lemma 4.3, we show that the last row is also invariant under σ, but this time we have to use the C-H Theorem on the second principal submatrix of A, i.e., on M.

The bottom row of C_1C_2 is given by the dot product of the two vectors in (24) without their top rows. Thus, in the bottom row of C_1C_2, we are missing $-PM^{k-2}Q$'s in the summations.

If we add these missing terms across the bottom row (starting with the left-most), that is, if we add:

$$-PM^{n-2}Q, -PM^{n-3}Q, \ldots, -PMQ, -PQ \tag{31}$$

to the entries in the bottom row, respectively, we can conclude by the above argument that the result is invariant under σ.

We have that $p_M(M) = 0$, so $-Pp_M(M)Q = 0$, and since $p_M = C_3C_4 \ldots C_n$, it follows that if we multiply the bottom row of C_1C_2, where the terms listed in (31) have been added, by $p_M = C_3C_4 \cdots C_n$, these terms will disappear.

Hence, to prove the invariance under σ of the bottom entry of $C_1C_2 \cdots C_n$, we first add the extra terms in (31) to the bottom row of C_1C_2, use the above argument to conclude the invariance of the resulting bottom row of C_1C_2 under σ (which does not affect $C_3C_4 \cdots C_n$), and then show that the extra terms disappear by $p_M(M) = 0$ (that is, by the Cayley-Hamilton Theorem applied to M).

It remains to point out how to formalize this proof in LAP, which means how to express that (29) is invariant under σ. What we do is show that (29) = (29′), where (29′) is σ(29). We show the equality by showing that there is a correspondence of terms, where the correspondence is given by the above pairing up, and by the fact that the summation in (29) and in (29′) is the same. □

Lemma 4.4 Let A be an $n \times n$ matrix, and let M_2 be the second principal submatrix of A. Then LAP proves the following implication: $p_{M_2}(M_2) = 0 \Longrightarrow \det(I_1A) = -\det(A)$. That is, LAP proves that if the C-H Theorem holds for M_2, then the determinant of A is alternating in the first and second rows.

Proof. To prove this Lemma, we use the machinery developed in the proof of the previous Lemma. First of all, we already showed that LAP proves that the entries in C_1C_2 are of the form given by (30) (C_1C_2 is a Toeplitz matrix, and (30) gives the entries in the first column, for rows $k \geq 3$; we are interested in the last row). As before, we let $M = M_2$ for readability.

Let τ be the transposition of the first two rows of A, so τ is given by:

$$\begin{aligned} a, b, c, d &\overset{\tau}{\mapsto} c, d, a, b \\ R, P &\overset{\tau}{\mapsto} P, R \\ S, Q, M_2 &\overset{\tau}{\mapsto} S, Q, M_2 \end{aligned}$$

and τ has the following effect on the term of (30):

$$\begin{aligned} -bPM^{k-2}S &\longmapsto -dRM^{k-2}S \\ -cRM^{k-2}Q &\longmapsto -aPM^{k-2}Q \\ +dRM^{k-3}S &\longmapsto +bPM^{k-3}S \\ +aPM^{k-3}Q &\longmapsto +cRM^{k-3}Q \\ +(PM^{k-4-i}Q)(RM^iS) &\longmapsto +(RM^{k-4-i}Q)(PM^iS) \\ -(RM^iQ)(PM^{k-4-i}S) &\longmapsto -(PM^iQ)(RM^{k-4-i}S) \\ -RM^{k-2}S &\longmapsto -PM^{k-2}S \\ -PM^{k-2}Q &\longmapsto -RM^{k-2}Q \end{aligned}$$

Note that except for the last two rows, all the the other terms in (30) have a corresponding term of opposite sign, under τ. The terms in the last two rows disappear when they are multiplied by $p_M = C_3C_4 \ldots C_n$, since $p_M(M) = 0$ by the C-H Theorem. $\square$

Lemma 4.5 Let A be an $n \times n$ matrix, and let M_{i+1} be the $(i+1)$-st principal submatrix of A. Then LAP proves the following implication: $p_{M_{i+1}}(M_{i+1}) = 0 \implies p_{(I_iAI_i)} = p_A$. That is, LAP proves that if the C-H Theorem holds for M_{i+1}, then $p_{I_iAI_i}$ and p_A have the same char polynomial.

Proof. See Figure 1, and note that if $i \geq n-1$ then M_{i+1} is not defined, but this is not a problem, since we do not need the C-H Theorem to prove $p_{I_{n-1}AI_{n-1}} = p_A$.

The case $i = 1$ is Lemma 4.3, so we can assume that $1 < i < n-1$.

Using the fact that $I_i^2 = I$, we have:

$$RM^jS = R(I_iI_i)M^j(I_iI_i)S = (RI_i)(I_iM^jI_i)(I_iS) = (RI_i)(I_iMI_i)^j(I_iS) \tag{32}$$

Here we use induction on j in the last step. The Basis Case is $j = 1$, so $I_iMI_i = I_iMI_i$ just by equality axioms. For the Induction Step, note that:

$$I_iM^{j+1}I_i = I_iM^jMI_i = I_iM^j(I_iI_i)MI_i = (I_iM^jI_i)(I_iMI_i)$$

and by the induction hypothesis, $I_iM^jI_i = (I_iMI_i)^j$, so we are done.

By Berkowitz's algorithm we know that the characteristic polynomial of A is given by the following product of matrices:

$$C_1C_2 \cdots C_{i-1}C_i \cdots C_n$$

Let $C_1'C_2' \cdots C_n'$ be the characteristic polynomial of I_iAI_i. There, we padded the matrices $C_1, \ldots, C_n$ with zeros to make them all of equal size, and we put them in one big matrix C. Then, by computing the n-th power of C, we obtain the iterated matrix product $C_1C_2 \cdots C_n$. Here, whenever we talk of iterated matrix products, we have this construction in mind.

Using Lemma 4.3 and $p_{M_{i+1}}(M_{i+1}) = 0$, we know that if we interchange the first two rows and the first two columns of M_{i-1} (which are contained in the i-th and $(i+1)$-st rows and columns of A), the characteristic polynomial of M_{i-1} remains invariant. This gives us:

$$C_i C_{i+1} \cdots C_n = C'_i C'_{i+1} \cdots C'_n \tag{33}$$

Now we are going to prove that for $1 \leq k \leq i-1$, $C_k = C'_k$. To see this, consider the first column of C'_k (it is enough to consider the first column as these are Toeplitz matrices). We are going to examine all the entries in this columns:

- The first entry is 1, which is a constant.
- The second entry is a_{kk}, just as in C_k since $k \leq i-1$.
- $R_k M_k^j S_k$ is replaced by $(R_k I_{i+1-k})(I_{i+1-k} M_k I_{i+1-k})^j (I_{i+1-k} S_k)$, but by (32) these two are equal. (Note that $0 \leq j \leq n-k-1$).

Thus, $C_k = C'_k$, for $1 \leq k \leq i-1$ and so $C_1 C_2 \cdots C_{i-1} = C'_1 C'_2 \cdots C'_{i-1}$. Combining this with (33) gives us:

$$C_1 C_2 \cdots C_n = C'_1 C'_2 \cdots C'_n$$

and so A and $I_i A I_i$ have the same characteristic polynomial, i.e., $p_{(I_i A I_i)} = p_A$. □

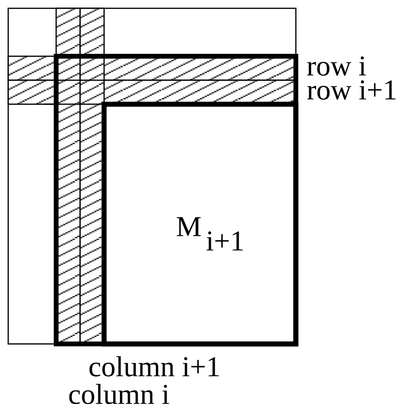

Figure 1: Matrix A: $p_{M_{i+1}}(M_{i+1}) = 0 \Longrightarrow p_{(I_i A I_i)} = p_A$

Corollary 4.1 Let A be an $n \times n$ matrix, and let $1 \leq i < j \leq n$. LAP proves, using the C-H Theorem on $(n-1) \times (n-1)$ matrices, that $p_{(I_{ij} A I_{ij})} = p_A$.

Proof. First of all, to prove this Corollary to Lemma 4.5, we are going to list explicitly the matrices for which we require the C-H Theorem: we need the following principal submatrices of A: $\{M_{i+1}, \ldots, M_j\}$ as well as the matrices $\{M'_{j-1}, \ldots, M'_{i+1}\}$ which are obtained from the corresponding principal submatrices, by replacing, in A, the j-th row by the i-th row, and the j-th column by the i-th column. The details are given in Figure 2.

To see why we require the C-H Theorem on precisely the matrices listed above, we illustrate how we derive $p_{(I_{13} A I_{13})} = p_A$ (see Figure 3). Using $p_{M_2}(M_2) = 0$ and Lemma 4.5 we interchange the first two rows (and the first two columns, but for clarity, we do not show the columns). Then,

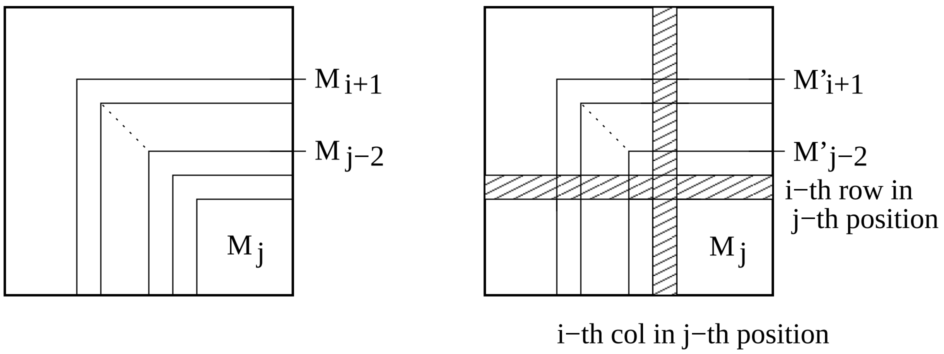

Figure 2: $\{M_{i+1}, \dots, M_j\}$ and $\{M'_{j-1}, \dots, M'_{i+1}\}$

using $p_{M_3}(M_3) = 0$ and Lemma 4.5, we interchange rows two and three, so at this point, the original row one is in position. We still need to take the original row three from position two to position one. This requires the use of $p_{M'_2}(M'_2) = 0$ and Lemma 4.5. The prime comes from the fact that what used to be row three, has now been replaced by row one. So using $p_{M'_2}(M'_2) = 0$, we exchange row two and one, and everything is in position.

Now the same argument, but in the general case, relies on the fact that:

$$I_{ij} = I_{i(i+1)} I_{(i+1)(i+2)} \cdots I_{(j-1)j} I_{(j-1)(j-2)} \cdots I_{(i+1)i} \tag{34}$$

i.e., any permutation can be written as a product of transpositions. Using Lemma 4.5 at each step, we are done. Equation (34) can be proven in LAP as follows: first note that $I_{ij} = I_{1i} I_{1j} I_{1i}$, so it is enough to prove that I_{1i} is equal to a product of transpositions, for any i.

We use induction on i. The **Basis Case** is $i = 2$, and I_{12} is a transposition, so there is nothing to prove. Now the **Induction Step**. Assume the claim holds for I_{1i}, and show that it holds for $I_{1(i+1)}$. This follows from the fact that $I_{1(i+1)} = I_{1i} I_{i(i+1)} I_{1i}$. □

Corollary 4.2 LAP proves, using the C-H Theorem, that det is alternating in the rows, i.e., $\det(A) = -\det(I_{ij}A)$.

Proof. Since $I_{ij} = I_{1i} I_{1j} I_{1i}$, it is enough to prove this for I_{1j}. If $j = 2$ we are done by Lemma 4.3. If $j > 2$, then use I_{2j} to bring the j-th row to the second position, and by Corollary 4.1, A and $I_{2j} A I_{2j}$ have the same char polynomials. Now apply I_{12} with Lemma 4.3, and use I_{2j} once again to put things back in order. □

Example 4.1 Suppose that we want to show that $\det(A) = -\det(I_{15}A)$. Consider:

$$A \xrightarrow{(1)} I_{25} A I_{25} \xrightarrow{(2)} I_{12} I_{25} A I_{25} \xrightarrow{(3)} I_{25} I_{12} I_{25} A I_{25} I_{25} = I_{15} A$$

By Corollary 4.1, (1) preserves the characteristic polynomial, and hence it also preserves the determinant. By Lemma 4.3, (2) changes the sign of the determinant. By Corollary 4.1 again, (3) preserves the determinant. Therefore, $\det(A) = -\det(I_{15}A)$.

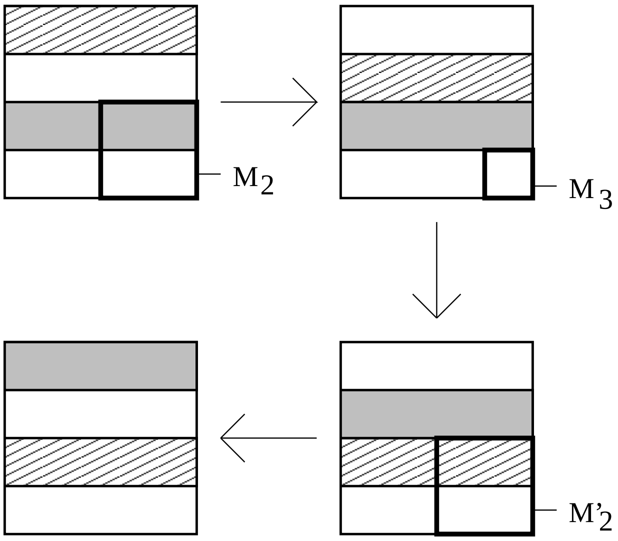

Figure 3: Example of $p_{(I_{13}AI_{13})} = p_A$

4.5 The cofactor expansion

We show that LAP proves that the cofactor expansion formula (22) follows from the axiomatic definition of the determinant. We first show that the cofactor expansion of A along the first row is equal to $\det(A)$. Define A_j, for $1 \leq j \leq n$, to be A, with the first row replaced by zeros, except for the $(1, j)$-th entry which remains unchanged. Then, using multilinearity along the first row of A, we obtain:

$$\det(A) = \det(A_1) + \det(A_2) + \cdots + \det(A_n) \tag{35}$$

Consider A_j, for $j > 1$. If we interchange the first column and the j-th column, and then, with $(j-2)$ transpositions we bring the first column (which is now in the j-th position) to the second position, we obtain, by alternation and (23), the following:

$$\begin{aligned}\det(A_j) &= (-1)^{j-1} a_{1j} \det(A[1|j]) \\ &= (-1)^{1+j} a_{1j} \det(A[1|j])\end{aligned}$$

Using this, and from equation (35), we obtain the cofactor expansion along the first row, that is, we obtain (22) for $i = 1$.

If we want to carry out the cofactor expansion along the i-th row (where $i > 1$), we interchange the first and the i-th row, and then we bring the first row (which is now in the i-th position) to the second row with $(i-2)$ transposition. Denote this new matrix A', and note that $\det(A') = (-1)^{i-1}\det(A)$. Now, expanding along the first row of A', we obtain (22) for $i > 1$.

4.6 The adjoint as a matrix of cofactors

We wish to show that LAP proves the C-H theorem from the cofactor expansion formula (i.e., from (22)). To this end, we first show that (22) implies (in LAP) the axiomatic definition of determinant.

We want to show that we can get multilinearity, alternation and $\det(I) = 1$ from (22). To show multilinearity along row (column) i, we just expand along row (column) i. To show $\det(I) = 1$

use induction on the size of I; in fact, showing that $\det(I) = 1$ can be done in LAP without any assumptions.

It is very easy to show that alternation follows from multilinearity and from:

$$\text{If two rows (columns) of } A \text{ are equal} \implies \det(A) = 0$$

To show this in LAP (from the cofactor expansion formula), we expand along row i first to obtain:

$$\det(A) = \sum_{k=1}^{n} (-1)^{i+k} a_{ik} \det(A[i|k])$$

and then we expand each minor $A[i|k]$ along the row that corresponds to the j-th row of A. Note that we end up with $n(n-1)$ terms; polynomially many in the size of A. Since row i is identical to the row j, we can pair each term with its negation; hence the result is zero, so $\det(A) = 0$.

Therefore, we have that the axiomatic definition of the determinant follows from the cofactor expansion formula, in LAP. We can now proceed, and finish showing the equivalences in Theorem 4.2, by showing that the cofactor expansion formula implies the C-H theorem, also in LAP.

Lemma 4.6 LAP proves that:

$$\operatorname{adj}(A) = ((-1)^{i+j} \det(A[j|i]))_{ij}$$

i.e., that $\operatorname{adj}(A)$ is the transpose of the matrix of cofactors of A, from the axiomatic definition of det.

Consider the following matrix:

$$C = \begin{pmatrix} 0 & e_i^t \\ e_j & A \end{pmatrix}$$

where e_i is a column vector with zeros everywhere except in the i-th position where it has a 1. By (23), we have that:

$$\det(C) = -e_i^t \operatorname{adj}(A) e_j = \ (i,j)\text{-th entry of } -\operatorname{adj}(A)$$

On the other hand, from alternation on C, we have that $\det(C) = (-1)^{i+j+1} \det(A[j|i])$. To see this, note that we need $(j+1)$ transpositions to bring the j-th row of A to the first row in the matrix C, to obtain the following matrix:

$$C' = \begin{pmatrix} 1 & A_j \\ 0 & e_i^t \\ 0 & A[j|-] \end{pmatrix}$$

where A_j denotes the j-th row of A, and $A[j|-]$ denotes A with the j-th row deleted. Then, by (23), we have:

$$\det(C') = \det \begin{pmatrix} e_i^t \\ A[j|-] \end{pmatrix}$$

and now with i transpositions, we bring the i-th column of $\begin{pmatrix} e_i^t \\ A[j|-] \end{pmatrix}$ to the first column, to obtain: $\begin{pmatrix} 1 & 0 \\ 0 & A[j|i] \end{pmatrix}$. Therefore, $\det(C') = (-1)^i \det(A[j|i])$ finishing the proof.

Therefore, LAP proves that the (i,j)-th entry of $\operatorname{adj}(A)$ is given by $(-1)^{i+j} \det(A[j|i])$.

Note that $p_A(A) = 0$ can also be stated as $A\text{adj}(A) = \det(A)I$, using our definitions of the adjoint and the determinant. Thus, the following shows that LAP proves the C-H theorem from the cofactor expansion formula: LAP proves $A\text{adj}(A) = \text{adj}(A)A = \det(A)I$ from the cofactor expansion formula.

We show first that $A\text{adj}(A) = \det(A)I$. The (i,j)-th entry of $A\text{adj}(A)$ is equal to:

$$a_{i1}(-1)^{j+1}\det(A[j|1]) + \cdots + a_{in}(-1)^{j+n}\det(A[j|n]) \tag{36}$$

If $i = j$, this is the cofactor expansion along the i-th row. Suppose now that $i \neq j$. Let A' be the matrix A with the j-th row replaced by the i-th row. Then, by alternation, $\det(A') = 0$. Now, (36) is the cofactor expansion of A' along the j-th row, and therefore, it is 0. This proves that $A\ \text{adj}(A) = \det(A)I$, and by definition of the adjoint, $\text{adj}(A)A = A\ \text{adj}(A)$, so we are done.

4.7 The multiplicativity of the determinant

The multiplicativity of the determinant is the property: $\det(AB) = \det(A)\det(B)$. This turns out to be a very strong property, from which all other properties follow readily in LAP.

Even the C-H theorem follows readily from the multiplicativity of det: from the multiplicativity of the determinant we have that $\det(I_{12}AI_{12}) = \det(I_1)\det(A)\det(I_1) = \det(A)$ for any matrix A. Suppose we want to prove the C-H theorem for some $n \times n$ matrix M. Define A as follows:

$$A = \begin{pmatrix} a & b & R \\ c & d & P \\ S & Q & M \end{pmatrix} = \begin{pmatrix} 0 & 0 & e_i^t \\ 0 & 0 & 0 \\ e_j & 0 & M \end{pmatrix}$$

Let $C_1C_2C_3\cdots C_{n+2}$ be the characteristic polynomial of A (and $C_3\cdots C_{n+2}$ the characteristic polynomial of M). From Berkowitz's algorithm it is easy to see that for A defined this way the bottom row of C_1C_2 is given by:

$$e_i^tM^ne_j \quad e_i^tM^{n-1}e_j \quad \ldots \quad e_i^tIe_j$$

so the bottom row of $C_1C_2C_3\cdots C_{n+2}$ is simply $e_i^tp(M)e_j$ where p is the characteristic polynomial of M.

On the other hand, using $\det(A) = \det(I_{12}AI_{12})$ and Berkowitz's algorithm, we have that:

$$\det(A) = \det\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & e_i^t \\ 0 & e_j & M \end{pmatrix} = 0$$

so that $e_i^tp(M)e_j = 0$, and since we can choose any i, j, we have that $p(M) = 0$.

What about the other direction? That is, can we prove the following implication in LAP:

$$\text{C-H theorem} \Longrightarrow \text{Multiplicativity of the determinant?}$$

The answer is "yes," *if* LAP can prove the following:

$$\det(A) = 0 \rightarrow AB \neq I \tag{37}$$

That is, LAP can prove the multiplicativity of the determinant from the C-H theorem and (37).

Theorem 4.3 LAP proves the multiplicativity of the determinant from the C-H Theorem and the property given by (37).

Proof. We prove the Lemma by induction on the size of the matrices; so assume that A, B are square $n \times n$ matrices. Since we assume the Cayley-Hamilton Theorem, by the results in the previous sections we also have at our disposal the cofactor expansion and the axiomatic definition of the determinant.

Suppose first that the determinants of all the minors of A (or B) are zero. Then, using the cofactor expansion we obtain $\det(A) = 0$. We now want to show that $\det(AB) = 0$ as well.

Suppose that $\det(AB) \neq 0$. Then, by the C-H Theorem, AB has an inverse C, i.e., $(AB)C = I$. But then $A(BC) = I$, so A is invertible, contrary to (37). Therefore, $\det(AB) = 0$, so that in this case $\det(A)\det(B) = \det(AB)$.

Suppose now that both A and B have a minor whose determinant is not zero. We can assume that it is the principal submatrix whose determinant is not zero (as A and $I_{1i}AI_{1j}$ have the same determinant, so we can bring any non-singular minor to be the principal minor). So assume that M_A, M_B are non-singular, where:

$$A = \begin{pmatrix} a & R_A \\ S_A & M_A \end{pmatrix} \qquad B = \begin{pmatrix} b & R_B \\ S_B & M_B \end{pmatrix}$$

By the Induction Hypothesis we know that $\det(M_A M_B) = \det(M_A)\det(M_B)$. Also note that:

$$AB = \begin{pmatrix} ab + R_A S_B & aR_B + R_A M_B \\ bS_A + M_A S_B & S_A R_B + M_A M_B \end{pmatrix}$$

Now using Berkowitz's algorithm:

$$\det(A)\det(B) = (a\det(M_A) - R_A \mathrm{adj}(M_A) S_A)(b\det(M_B) - R_B \mathrm{adj}(M_B) S_B) \tag{38}$$

We want to show that $\det(AB)$ is equal to (38). Again, using Berkowitz's algorithm:

$$\begin{aligned} \det(AB) &= (ab + R_A S_B)\det(S_A R_B + M_A M_B) \\ &\quad - (aR_B + R_A M_B)\mathrm{adj}(S_A R_B + M_A M_B)(bS_A + M_A S_B) \end{aligned} \tag{39}$$

We now show that the right hand sides of (38) and (39) are equal.

By Lemma 4.7:

$$\det(S_A R_B + M_A M_B) = \det(M_A M_B) + R_B \mathrm{adj}(M_A M_B) S_A \tag{40}$$

Using the IH, $\det(M_A M_B) = \det(M_A)\det(M_B)$, and using Lemma 4.6 and $\det(M_A) \neq 0$ and $\det(M_B) \neq 0$ we obtain: $\mathrm{adj}(M_A M_B) = \mathrm{adj}(M_B)\mathrm{adj}(M_A)$. To see this note that by the C-H Theorem $(M_A M_B)\mathrm{adj}(M_A M_B) = \det(M_A M_B) I$. We now multiply both sides of this equation by $\mathrm{adj}(M_A)$ to obtain, by the C-H Theorem again, $\det(M_A) M_B \mathrm{adj}(M_A M_B) = \det(M_A M_B)\mathrm{adj}(M_A)$. Now multiply both sides by $\mathrm{adj}(M_B)$ to obtain:

$$\det(M_A)\det(M_B)\mathrm{adj}(M_A M_B) = \det(M_A M_B)\mathrm{adj}(M_B)\mathrm{adj}(M_A)$$

Since $\det(M_A M_B) = \det(M_A)\det(M_B)$, and $\det(M_A)\det(M_B) \neq 0$, we obtain our result.

Therefore, from (40) we obtain:

$$\det(S_A R_B + M_A M_B) = \det(M_A)\det(M_B) + R_B \mathrm{adj}(M_B)\mathrm{adj}(M_A) S_A \tag{40$'$}$$

Using Lemma 4.8 and $\mathrm{adj}(M_A M_B) = \mathrm{adj}(M_B)\mathrm{adj}(M_A)$, we obtain:

$$\begin{aligned} R_B \mathrm{adj}(S_A R_B + M_A M_B) &= R_B \mathrm{adj}(M_B)\mathrm{adj}(M_A) \\ \mathrm{adj}(S_A R_B + M_A M_B) S_A &= \mathrm{adj}(M_B)\mathrm{adj}(M_A) S_A \end{aligned} \tag{41}$$

Finally, we have to prove the following identity:

$$\begin{aligned} R_A M_B \mathrm{adj}(S_A R_B + M_A M_B) M_A S_B = & \\ & R_A S_B \det(M_A)\det(M_B) - R_B \mathrm{adj}(M_B) S_B R_A \mathrm{adj}(M_A) S_A \\ & + (R_A S_B) R_B \mathrm{adj}(M_B)\mathrm{adj}(M_A) S_A \end{aligned} \tag{42}$$

First of all, by Lemma 4.6 we have:

$$(S_A R_B + M_A M_B)\mathrm{adj}(S_A R_B + M_A M_B) = \det(S_A R_B + M_A M_B)$$

Using Lemmas 4.7 and 4.8, we get:

$$S_A R_B \mathrm{adj}(M_A M_B) + M_A M_B \mathrm{adj}(S_A R_B + M_A M_B) = (\det(M_A M_B) + R_B \mathrm{adj}(M_A M_B) S_A) I$$

We have already shown above that $\mathrm{adj}(M_A M_B) = \mathrm{adj}(M_B)\mathrm{adj}(M_A)$ using our Induction Hypothesis: $\det(M_A M_B) = \det(M_A)\det(M_B)$. So, if we multiply both sides of the above equation by $\mathrm{adj}(M_A)$ on the left, and by M_A on the right, we obtain:

$$\begin{aligned} \mathrm{adj}(M_A) S_A R_B \mathrm{adj}(M_B)\det(M_A) + \det(M_A) M_B \mathrm{adj}(S_A R_B + M_A M_B) M_A = & \\ \det(M_A)(\det(M_A)\det(M_B) + R_B \mathrm{adj}(M_B)\mathrm{adj}(M_A) S_A) I & \end{aligned}$$

Since by assumption $\det(M_A) \neq 0$, we can divide both sides of the equation by $\det(M_A)$ to obtain:

$$\begin{aligned} \mathrm{adj}(M_A) S_A R_B \mathrm{adj}(M_B) + M_B \mathrm{adj}(S_A R_B + M_A M_B) M_A = & \\ (\det(M_A)\det(M_B) + R_B \mathrm{adj}(M_B)\mathrm{adj}(M_A) S_A) I & \end{aligned}$$

If we now multiply both sides of the above equation, by R_A on the left, and by S_B on the right, we obtain (42) as desired.

We now substitute ($40'$), (41), and (42) into (39), and we obtain that the right hand side of (39) is equal to the right hand side of (38), and we are done. □

Lemma 4.7 LAP proves, from the axiomatic definition of det, that:

$$\det(SR + M) = \det(M) + R\ \mathrm{adj}(M)\ S \tag{43}$$

Proof. Consider the matrices C and C', where C' is obtained from C by adding multiples of the first row of C to clear its first column:

$$C = \left(\begin{array}{c|c} 1 & -R \\ \hline S & M \end{array}\right) \quad \text{and} \quad C' = \left(\begin{array}{c|c} 1 & -R \\ \hline 0 & SR + M \end{array}\right)$$

By Lemma 4.1, $\det(C) = \det(M) + R\ \mathrm{adj}(M)\ S$. By the axiomatic definition of det, we have that $\det(C') = \det(C)$. Using Lemma 4.1 on C', we obtain: $\det(C') = \det(SR + M)$, and hence the result follows. □

Lemma 4.8 LAP proves, from the Cayley-Hamilton Theorem, that:

$$\begin{aligned} R\mathrm{adj}(SR + M) &= R\mathrm{adj}(M) \\ \mathrm{adj}(SR + M)S &= \mathrm{adj}(M)S \end{aligned}$$

Proof. By Lemma 4.6 we know that $\mathrm{adj}(A)$ is the transpose of the matrix of cofactors of A. From this we can deduce the following identity:

$$\mathrm{adj}(A) = \begin{pmatrix} \det(M) & -R\mathrm{adj}(M) \\ -\mathrm{adj}(M)S & (1+a_{11})\mathrm{adj}(M) - \mathrm{adj}(SR+M) \end{pmatrix} \tag{44}$$

To see this we are going to consider the four standard submatrices. First of all, the $(1,1)$ entry of $\mathrm{adj}(A)$ is the determinant of the principal minor of A times $(-1)^{1+1}$, i.e. $\det(M)$. The remaining entries along the first row are given by $(-1)^{1+i}\det(A[i|1])$, for $2 \leq i \leq n$. Note that for $2 \leq i \leq n$, $A[i|1]$ is given by:

$$\begin{pmatrix} R \\ M[i|-] \end{pmatrix} \tag{45}$$

where $M[i|-]$ denotes M without the i-th row. To compute the determinant of the matrix given by (45) expand along the first row to obtain: $\sum_{j=1}^{n-1} r_j(-1)^{i+j}\det(M[i|j])$. This gives us $-R\mathrm{adj}(M)$ as desired. In the same way we can show that the entries in the first column below $(1,1)$ are given by $-\mathrm{adj}(M)S$.

We now show that the principal submatrix is given by $(1+a_{11})\mathrm{adj}(M) - \mathrm{adj}(SR+M)$. To see this first note that $(SR+M)[i|j] = S[i]R[j] + M[i|j]$, where $S[i], R[j]$ denote S, R without the i-th row and j-th column, respectively. Now using Lemma 4.7 we have that $\det((SR+M)[i|j]) = \det(M[i|j]) + R[j]\mathrm{adj}(M[i|j])S[i]$. The $(i+1, j+1)$ entry of $\mathrm{adj}(A)^t$, $1 \leq i,j < n$, is given by:

$$(-1)^{i+j}(a_{11}\det(M[i|j]) - R[j]\mathrm{adj}(M[i|j])S[i])$$

as can be seen from Figure 4.

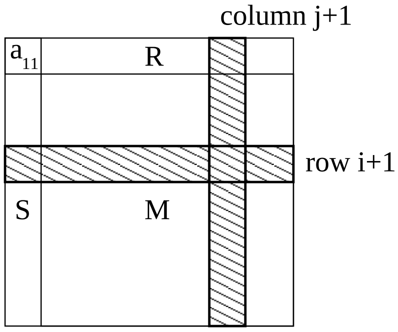

Figure 4: Showing that $\mathrm{adj}(A)[1|1] = (1+a_{11})\mathrm{adj}(M) - \mathrm{adj}(SR+M)$

Therefore, the $(i+1, j+1)$ entry of $\mathrm{adj}(A)^t$ is given by:

$$(-1)^{i+j}(a_{11}\det(M[i|j]) + \det(M[i|j]) - \det((SR+M)[i|j]))$$

and we are done.

By Lemma 4.6 we know that:

$$\begin{pmatrix} a_{11} & R \\ S & M \end{pmatrix} \begin{pmatrix} \det(M) & -R\mathrm{adj}(M) \\ -\mathrm{adj}(M)S & (1+a_{11})\mathrm{adj}(M) - \mathrm{adj}(SR+M) \end{pmatrix} = \det(A)I$$

In particular this means that:

$$-a_{11}R\mathrm{adj}(M) + R(1+a_{11})\mathrm{adj}(M) - R\mathrm{adj}(SR+M) = 0$$

and from this it follows that $R\mathrm{adj}(SR+M) = R\mathrm{adj}(M)$. Similarly, we can prove the second identity. □

5 The theory $\forall$LAP

We extend the theory LAP to $\forall$LAP, where we allow induction over formulas with a bounded universal matrix quantifier. We show that $\forall$LAP proves the C-H Theorem, and the multiplicativity of det. By Theorem 4.2, it follows that $\forall$LAP also proves the axiomatic definition of det, and the cofactor expansion formula. All of these results continue to hold when the underlying field is replaced by an arbitrary commutative ring.

As discussed in section 6, proofs in $\forall$LAP are feasible, in the sense that they require only polynomial time concepts. It follows that all the principles of linear algebra listed in Theorem 4.2 have feasible proofs. We believe that we give the first feasible proofs of these principles.

We define Π_0^M to be the set of formulas over $\mathcal{L}_{\text{LAP}}$ ("M" stands for matrix). We define Π_1^M to be the set of formulas in Π_0^M together with formulas of the form $(\forall A \leq n)\alpha$, where $\alpha \in \Pi_0^M$, and where $(\forall A \leq n)\alpha$ abbreviates:

$$(\forall A)((\mathtt{r}(A) \leq n \wedge \mathtt{c}(A) \leq n) \supset \alpha)$$

where A is a matrix variable, *not* contained in the index term n.

We define the system $\forall$LAP to be similar to LAP, but we allow Π_1^M formulas. The underlying logic is again based on Gentzen's sequent system LK. Whereas LAP needs only the propositional rules of LK, we now need the rules for introducing a universal quantifier on the left and on the right of a sequent:

$$\text{left} \quad \frac{\mathtt{r}(T) \leq n, \mathtt{c}(T) \leq n, \alpha(T), \Gamma \rightarrow \Delta}{(\forall X \leq n)\alpha(X), \Gamma \rightarrow \Delta}$$

$$\text{right} \quad \frac{\mathtt{r}(A) \leq n, \mathtt{c}(A) \leq n, \Gamma \rightarrow \Delta, \alpha(A)}{\Gamma \rightarrow \Delta, (\forall X \leq n)\alpha(X)}$$

where T is any term of type matrix, and n is any term of type index. Also, in $\forall$-introduction-right, A is a variable of type matrix that does not occur in the lower sequent, **and** in both rules α is a Π_0^M formula, because we just want (need) a single matrix quantifier.

The main observation is that in $\forall$LAP we can use the induction rule over Π_1^M formulas. It is this strengthening which finally allows us to prove all the principles listed in Theorem 4.2.

None of the results in this section requires inverses of field elements, and hence all results hold over any commutative ring.

5.1 $\forall$LAP proves the C-H Theorem

The basic idea behind the proof is the following: if $p_A(A) \neq 0$, that is, if the C-H theorem fails for A, then we can find (*in polytime*) a sub-matrix B of A for which $p_B(B) \neq 0$, i.e., for which the C-H theorem fails already. Since the C-H Theorem does *not* fail for 1×1 matrices, after at most $n =$ (size of A) steps we get a contradiction. This idea can be expressed with universal quantifiers over variables of type matrix: if the C-H theorem holds for all matrices smaller than A, then it also holds for A. The matrix B is obtained from A by selecting an index i such that column i of $p_A(A)$ is nonzero, and interchanging the first row and column of A with the i-th row and column, respectively, and finally deleting the first row and column of the result. Lemma 5.1 below guarantees that $p_B(B) \neq 0$.

Theorem 5.1 $\forall$LAP (over any commutative ring) proves the C-H theorem.

Proof. We prove that for all $n \times n$ matrices A, $p_A(A) = 0$, by induction on n. The **Basis Case** is trivial: if $A = (a_{11})$, then the characteristic polynomial of A is $x - a_{11}$. We use the following strong induction hypothesis: $(\forall A \leq n)p_A(A) = 0$. Thus, in our **Induction Step** we prove:

$$(\forall M \leq n)p_M(M) = 0 \to (\forall A \leq n+1)p_A(A) = 0 \tag{46}$$

Let A be an $(n+1) \times (n+1)$ matrix, and assume that we have $(\forall M \leq n)p_M(M) = 0$. By Corollary 4.1 we have that for all $1 \leq i < j \leq n+1$, $p_{(I_{ij}AI_{ij})} = p_A$. Suppose, for the sake of contradiction, that the i-th column of $p_A(A)$ is *not* zero. Then, the first column of $I_{1i}p_A(A)I_{1i}$ is not zero. But:

$$I_{1i}p_A(A)I_{1i} = p_A(I_{1i}AI_{1i}) = p_{(I_{1i}AI_{1i})}(I_{1i}AI_{1i})$$

Let $C = I_{1i}AI_{1i}$. By the induction hypothesis, $p_{C[1|1]}(C[1|1]) = 0$. By Lemma 5.1 below, the first column of $p_C(C)$ is zero; therefore, the first column of $p_{(I_{1i}AI_{1i})}(I_{1i}AI_{1i})$ *is* zero. Contradiction. $\Box$

Lemma 5.1 LAP proves that if $p_{C[1|1]}(C[1|1]) = 0$, then the first column of $p_C(C)$ is zero.

Proof. We restate the Lemma using the usual notation of A and $M = A[1|1]$, where A is an $n \times n$ matrix, $n > 1$. Thus, we want to show that LAP proves the following: if $p_M(M) = 0$, then the first column of $p_A(A)$ is zero. We let $p = p_A$ and $q = p_M$, that is, p, q are the characteristic polynomials of $A, M = A[1|1]$, respectively. Define w_k, X_k, Y_k, Z_k as follows:

$$A = \begin{pmatrix} w_1 & X_1 \\ Y_1 & Z_1 \end{pmatrix} = \begin{pmatrix} a_{11} & R \\ S & M \end{pmatrix}$$
$$A^{k+1} = \begin{pmatrix} w_{k+1} & X_{k+1} \\ Y_{k+1} & Z_{k+1} \end{pmatrix} = \begin{pmatrix} w_k & X_k \\ Y_k & Z_k \end{pmatrix} \begin{pmatrix} a_{11} & R \\ S & M \end{pmatrix} \quad \text{for } k \geq 1$$

It is easy to see that LAP proves the following equations:

$$\begin{aligned} w_{k+1} &= a_{11}w_k + X_kS \\ X_{k+1} &= w_kR + X_kM \\ Y_{k+1} &= a_{11}Y_k + Z_kS \\ Z_{k+1} &= Y_kR + Z_kM \end{aligned} \tag{47}$$

Using Berkowitz's algorithm (14,15), it is not hard to show in LAP that:

$$p(A) = (A - a_{11}I)q(A) - \sum_{k=1}^{n-1} q_k \sum_{i=0}^{k-1}(RM^iS)A^{k-1-i} \tag{48}$$

and thus, to show that the first column of $p(A)$ is zero, it is enough to show that the first columns of $(A - a_{11}I)q(A)$ and $\sum_{k=1}^{n-1} q_k \sum_{i=0}^{k-1}(RM^iS)A^{k-1-i}$ are the same. This is the strategy for proving Claims 5.1 and 5.2, which will establish the Lemma.

Claim 5.1 The upper-left entry of $p(A)$ is zero.

Proof. If we make the convention $w_0 = 1$, then using the second line of (47) we can prove by induction on k:

$$X_k = \sum_{i=0}^{k-1} w_{k-1-i}RM^i, \text{for } k \geq 1$$

Using this and the first line of (47) we obtain

$$\begin{cases} w_0 = 1 \\ w_1 = a_{11} \\ w_{k+1} = a_{11}w_k + \sum_{i=0}^{k-1}(RM^iS)w_{k-1-i}, \text{for } k \geq 1 \end{cases} \tag{49}$$

The top left entry of $(A - a_{11}I)q(A)$ is given by

$$\sum_{k=1}^{n-1} q_k(w_{k+1} - a_{11}w_k) \tag{50}$$

(notice that we can ignore the term $k = 0$ since the top left entry of A is the same as the top left entry of $a_{11}I$). We can compute $(w_{k+1} - a_{11}w_k)$ using the recursive definitions of w_k (given by (49) above):

$$w_{k+1} - a_{11}w_k = a_{11}w_k + \sum_{i=0}^{k-1}(RM^iS)w_{k-1-i} - a_{11}w_k = \sum_{i=0}^{k-1}(RM^iS)w_{k-1-i}$$

Thus, (50) is equal to

$$\sum_{k=1}^{n-1} q_k \sum_{i=0}^{k-1}(RM^iS)w_{k-1-i}$$

This proves that the top left entry of $p(A)$ is zero (see equation (48) and the explanation below it). □

Claim 5.2 The $(n-1) \times 1$ lower-left submatrix of $p(A)$ is zero.

Proof. Using the last line of (47) we can prove by induction on k

$$Z_k = M^k + \sum_{i=0}^{k-2} Y_{k-1-i}RM^i, \text{for } k \geq 2$$

Using this and the second last line of (47), if we make the convention $Y_0 = 0$ then

$$\begin{cases} Y_0 = 0 \\ Y_1 = S \\ Y_{k+1} = a_{11}Y_k + M^kS + \sum_{i=0}^{k-2}(RM^iS)Y_{k-1-i}, \text{for } k \geq 1 \end{cases} \tag{51}$$

(Note that RM^iS is a scalar.) The lower-left $(n-1) \times 1$ submatrix of $(A - a_{11}I)q(A)$ is given by

$$\sum_{k=0}^{n-1} q_k(Y_{k+1} - a_{11}Y_k)$$

and by (51) we have that for $k \geq 2$, $Y_{k+1} - a_{11}Y_k$ is given by:

$$\left(a_{11}Y_k + M^kS + \sum_{i=0}^{k-2}(RM^iS)Y_{k-1-i}\right) - a_{11}Y_k = M^kS + \sum_{i=0}^{k-2}(RM^iS)Y_{k-1-i}$$

ans, therefore, $\sum_{k=0}^{n-1} q_k(Y_{k+1} - a_{11}Y_k)$ is given by:

$$
\begin{aligned}
& q_0(Y_1 - a_{11}Y_0) + q_1(Y_2 - a_{11}Y_1) + \sum_{k=2}^{n-1} q_k \left(M^k S + \sum_{i=0}^{k-2} (RM^iS)Y_{k-1-i} \right) \\
&= q(M)S + \sum_{k=2}^{n-1} q_k \sum_{i=0}^{k-2} (RM^iS)Y_{k-1-i}
\end{aligned}
$$

where we have used the facts $Y_0 = 0$, $Y_1 = S$, and $Y_2 = a_{11}S + MS$. Now by assumption $q(M) = 0$, so we can conclude that:

$$
\sum_{k=0}^{n-1} q_k(Y_{k+1} - a_{11}Y_k) = \sum_{k=1}^{n-1} q_k \sum_{i=0}^{k-1} (RM^iS)Y_{k-1-i} \tag{52}
$$

The RHS of (52) is equal to the $(n-1) \times 1$ lower-left submatrix of $\sum_{k=1}^{n-1} q_k \sum_{i=0}^{k-1} (RM^iS)A^{k-1-i}$, and hence the claim follows (once again, see equation (48) and the explanation below it). □

This ends the proof of the Lemma 5.1. □

Corollary 5.1 $\forall$LAP (over any commutative ring) proves the axiomatic definition of det, and the cofactor expansion formula.

Proof. By Theorem 4.2, the C-H Theorem is equivalent to the axiomatic definition of det, and the cofactor expansion formula, and furthermore, this equivalence can be proven in LAP. □

5.2 $\forall$LAP proves the multiplicativity of det

Theorem 5.2 $\forall$LAP (over any commutative ring) proves the multiplicativity of det.

Proof. To show the multiplicativity of det in $\forall$LAP, we use two principles which can be proven in $\forall$LAP by the results of the previous section:

- The cofactor expansion formula for det (along rows *and* columns),
- and the axiomatic definition of det, from which it follows (easily) that if we add a multiple of one row to another row, the determinant remains invariant.

Our proof is by induction on the size of matrices, and the Basis Case, 1×1 matrices, is trivial. Next, we show the Induction Step, where we prove, using the cofactor expansion formula along rows and columns, and using the axiomatic definition of det, that if multiplicativity holds for $(n-1) \times (n-1)$ matrices, it also holds for $n \times n$ matrices.

So suppose that A, B are $n \times n$ matrices, and so is $C = AB$. Using the multilinearity of det along the first column of C, $\forall$LAP proves

$$
\begin{aligned}
\det(C) &= \det(C_1, C_2, \ldots, C_n) \\
&= \det(b_{11}A_1 + b_{21}A_2 + \cdots + b_{n1}A_n, C_2, \ldots, C_n) \\
&= \sum_{k=1}^{n} \det(b_{k1}A_k, C_2, \ldots, C_n)
\end{aligned}
$$

where C_i denotes the i-th column of C, and A_i denotes the i-th column of A.

Since adding a multiple of one row to another row does not change det, $\forall$LAP proves for $1 \leq k \leq n$

$$\det(A_k, C_2, \ldots, C_n) = \det(A_k, C_2 - b_{k2}A_k, \ldots, C_n - b_{kn}A_k)$$

and hence by linearity $\forall$LAP proves

$$\det(b_{k1}A_k, C_2, \ldots, C_n) = \det(b_{k1}A_k, C_2 - b_{k2}A_k, \ldots, C_n - b_{kn}A_k) \tag{53}$$

Notice, that the matrix given by $(C_2 - b_{k2}A_k, \ldots, C_n - b_{kn}A_k)$ with the l-th row removed is just $A[l|k]B[k|1]$. Thus, using the cofactor expansion along the first column of (53), we obtain for $1 \leq k \leq n$

$$(53) = \sum_{l=1}^{n} (-1)^{1+l} b_{k1} a_{lk} \det(A[l|k]B[k|1]) \tag{54}$$

We can now apply the induction hypothesis to (54) to conclude that for all l,

$$\det(A[l|k]B[k|1]) = \det(A[l|k]) \det(B[k|1])$$

Notice that it is here where we see that we need $\forall$-induction (and hence $\forall$LAP, not just LAP), because we have to apply the induction hypothesis to n different matrices, of size $(n-1) \times (n-1)$.

Thus, putting everything together we get:

$$\det(AB) = \det(C) = \sum_{k=1}^{n} \sum_{l=1}^{n} (-1)^{1+l} b_{k1} a_{lk} \det(A[l|k]) \det(B[k|1])$$

note that $(-1)^{1+l} = (-1)^{1+l+2k} = (-1)^{l+k}(-1)^{1+k}$, so:

$$= \sum_{k=1}^{n} \left((-1)^{1+k} b_{k1} \det(B[k|1]) \left(\sum_{l=1}^{n} (-1)^{l+k} a_{lk} \det(A[l|k]) \right) \right)$$

where $\sum_{l=1}^{n} (-1)^{l+k} a_{lk} \det(A[l|k])$ is the cofactor expansion of $\det(A)$ on the k-th column of A,

$$= \det(A) \sum_{k=1}^{n} (-1)^{1+k} b_{k1} \det(B[k|1])$$

where $\sum_{k=1}^{n} (-1)^{1+k} b_{k1} \det(B[k|1])$ is the cofactor expansion of $\det(B)$ along the first column of B, so:

$$= \det(A) \det(B)$$

and we are done. □

Corollary 5.2 $\forall$LAP (over any commutative ring) proves the hard matrix identities of section 3.1.

Proof. By using the multiplicativity of the determinant we can eliminate the use of field inverses in the proof of Theorem 4.1. Again, it suffices to consider the identity III:

$$AB = I \to BA = I$$

Assuming $AB = I$, we have by multiplicativity

$$\det(A)\det(B) = \det(I) = 1$$

and therefore $d = \det(A)$ is a unit in the underlying ring. By Theorem 5.1 we may assume the C-H theorem, and hence from (20) we have

$$\mathrm{adj}(A)A = d\ I$$

Using the assumption $AB = I$ we have $\mathrm{adj}(A)AB = \mathrm{adj}(A)$ and hence $B = d^{-1}\mathrm{adj}(A)$. Thus $BA = d^{-1}\mathrm{adj}(A)A = I$ as required. □

6 Propositional Translations and Feasible Proofs

The hard matrix identities (section 3.1) such as

$$AB = I \rightarrow BA = I \tag{55}$$

over the field of two elements translate naturally into a polynomial size family $\langle \mathrm{INV}_n \rangle$ of propositional tautologies. For each $n \geq 1$, the tautology INV_n expresses (55) when A and B are $n \times n$ matrices over $\mathbb{Z}_2$. In fact, INV_n is easily constructed from the $2n^2$ propositional variables a_{ij} and $b_{ij}, 1 \leq i, j \leq n$ representing the entries of A and B, respectively. This idea generalizes to all formulas α of LA, and the underlying field (or commutative ring) K does not have to be $\mathbb{Z}_2$, as long as it can be feasibly represented. It turns out (Theorem 6.3) that if α is a theorem of LA, then the corresponding tautology family has polynomial size proofs in an appropriate propositional proof system, depending on the underlying field. Similar results hold for LAP and $\forall\mathsf{LAP}$.

6.1 Complexity classes and their associated proof systems

Before giving details of the translation we give a brief review of propositional proof complexity (see [Kra95, Urq95]).

In the general sense, a propositional proof system can be regarded as a polynomial time map F from the set $\{0,1\}^*$ of strings onto the set of propositional tautologies. The idea here is that if π is an F-proof of a tautology A then $F(\pi) = A$.

Consider for example the system PK (which is Gentzen's sequent system LK restricted to propositional formulas). We can think of a PK proof of A as a sequence of sequents, each of which is either an axiom of the form $B \rightarrow B$ or follows from earlier sequents by a rule of inference, ending in the sequent $\rightarrow A$. The corresponding polynomial time function F_{PK} satisfies $F_{PK}(\pi) = A$, where π is a string coding such a PK proof.

A *Frege system* is a propositional proof system P such that a P-proof of a propositional formula A is (or codes) a finite sequence of formulas ending in A, each formula of which either is an axiom or follows from earlier formulas by a rule of inference. Further, axioms and rules are defined as substitution instances of finitely many schemes, and the system is required to be sound and implicationally complete. Most specific propositional proof systems described in logic texts are Frege systems, or are equivalent to Frege systems.

We say that a system $S2$ *p-simulates* a system $S1$ (written $S1 \leq_p S2$) if there is a polynomial time transformation which takes every $S1$ proof to a $S2$ proof of the same tautology. (In case the proof systems apply to tautologies with different connective sets, the tautologies must be translated in an appropriate way.) Two systems are *p-equivalent* if each p-simulates the other. It can be shown that any two Frege systems are p-equivalent to each other and to the system PK.

We say that a propositional proof system F is *polynomially bounded* if there is polynomial $p(n)$ such that every tautology A has an F-proof π of A (so $F(\pi) = A$) and $|\pi| \leq p(|A|)$, where $|x|$

indicates the length of a string x. It is not hard to show that a polynomially-bounded proof system exists iff $\mathbf{NP} = \mathbf{coNP}$ (i.e. iff the complement of every problem in $\mathbf{NP}$ is again in $\mathbf{NP}$). Because of this, a common conjecture is that no propositional proof system is polynomially-bounded.

Despite this conjecture, no one has even been able to prove that Frege systems are not polynomially bounded.

Many propositional proof systems are naturally associated with complexity classes. In particular, Frege systems are associated with the class $\mathbf{NC}^1$. Here a language $L \subseteq \{0,1\}^*$ in $\mathbf{NC}^1$ is specified by a polynomial size family $\langle B_n \rangle$ of propositional formulas, where B_n has variables $x_1, ..., x_n$, and a string of length n is in L iff it is the characteristic vector of a truth assignment satisfying B_n. The reason for associating Frege systems with $\mathbf{NC}^1$ is that the formulas in a polynomial size family of Frege proofs of a tautology family $\langle A_n \rangle$ can express concepts in $\mathbf{NC}^1$. For example, PHP_n is a well-studied propositional tautology expressing the fact that $n+1$ pigeons cannot fit in n holes unless at least one hole has two or more pigeons (the pigeonhole principle). Buss [Bus87] showed that $\langle \mathrm{PHP}_n \rangle$ has polynomial size Frege proofs, using the fact that counting the number of ones in an input string $x_1...x_n$ is an $\mathbf{NC}^1$ concept.

The complexity classes of interest in this paper form the chain

$$\mathbf{AC}^0 \subseteq \mathbf{AC}^0(2) \subseteq \mathbf{TC}^0 \subseteq \mathbf{NC}^1 \subseteq \mathbf{NC}^2 \subseteq \mathbf{P/poly} \tag{56}$$

A language in $\mathbf{AC}^0$ is specified by a polynomial size family of propositional formulas as for $\mathbf{NC}^1$, except now the alternation depth of $\wedge$ and $\vee$ in the family must be bounded by a constant. The class $\mathbf{AC}^0(2)$ is defined similarly, except now we allow parity subformulas $(x_1 \oplus x_2 \oplus ... \oplus x_n)$ asserting that the number of ones in $x_1, ..., x_n$ is odd, and again require that the depth of the formulas (with unbounded fanin $\wedge, \vee$, and $\oplus$) is bounded. The class $\mathbf{TC}^0$ is defined similarly except now we allow threshold gates $T_k(x_1, ..., x_n)$ asserting that at least k of $x_1, ..., x_n$ are ones. A language in $\mathbf{NC}^2$ is specified by a polynomial size family of Boolean circuits of depth bounded by $O((\log n)^2)$. A language in $\mathbf{P/poly}$ is specified by a polynomial size family of Boolean circuits (with no depth restriction). This is a nonuniform version of the class $\mathbf{P}$ of polynomial time languages. One can show that a language L is in $\mathbf{P/poly}$ iff there is a polynomial time Turing machine M and a polynomial size sequence $\langle v_n \rangle$ of "advice" strings such that a string w of length n is in L iff M accepts the input pair $\langle w, v_n \rangle$.

The corresponding propositional proof systems form a sequence

$$\mathbf{AC}^0\text{-Frege} \leq_p \mathbf{AC}^0(2)\text{-Frege} \leq_p \mathbf{TC}^0\text{-Frege} \leq_p \text{Frege} \leq_p \mathbf{NC}^2\text{-Frege} \leq_p \text{eFrege} \tag{57}$$

Here an $\mathbf{AC}^0$-Frege system is the same as a Frege system, except the $(\wedge, \vee)$ alternation depth of all formulas in a proof must be bounded by some fixed constant. The systems $\mathbf{AC}^0(2)$-Frege and $\mathbf{TC}^0$-Frege have a similar relation to the complexity classes $\mathbf{AC}^0(2)$ and $\mathbf{TC}^0$. An eFrege (extended Frege) proof is the same as a Frege proof, except a line $p \leftrightarrow B$ (defining the variable p) is allowed to appear in the proof for any formula B not containing p, provided that p does not occur earlier in the proof and does not occur in the conclusion. The idea is that each variable p corresponds to a gate in a Boolean circuit, and hence eFrege systems correspond to the complexity class $\mathbf{P/poly}$. The system $\mathbf{NC}^2$-Frege can be defined similarly by limiting the nesting depth of variable definitions $p \leftrightarrow B$ to $O(\log n)$.

Ajtai [Ajt88] proved that the pigeonhole tautologies $\langle \mathrm{PHP}_n \rangle$ do not have polynomial size $\mathbf{AC}^0$-Frege proofs, and hence no $\mathbf{AC}^0$-Frege system is polynomially bounded. However it is not known whether any proof system in the other classes described above is polynomially bounded.

One way to prove that Frege systems are not super might be to show that some specific tautology family, such at the translations $\langle \mathrm{INV}_n \rangle$ of the hard matrix identity (55), does not have polynomial size Frege proofs. This example is motivated by the intuition that proofs of these tautologies seem to require concepts (such as matrix inverse) that are not in $\mathbf{NC}^1$.

6.2 The systems PK(2) and $\mathbf{PK}_{BD}(2)$

Formulas in the propositional sequent system PK(2) are built from propositional variables $p, q, r, \ldots$ using the logical constants $\mathtt{F}$ and $\mathtt{T}$ (for false and true), the unary connective $\neg$, and the binary connectives $\wedge, \vee, \oplus$ (as well as parentheses). Here $\oplus$ represents exclusive or. An axiom is the sequent $\mathtt{F} \rightarrow$, or $\rightarrow \mathtt{T}$, or any sequent of the form $A \rightarrow A$, where A is a formula. The rules include the usual structural rules for LK, namely Exchange, Contraction, and Weakening (left and right), as well as the Cut rule and rules for introducing each of the connectives $\neg, \wedge, \vee, \oplus$ on the left and right (see [Bus98]). In particular, the rules for introducing $\oplus$ are

$$\textbf{left}\ \frac{\Gamma, \alpha \rightarrow \beta, \Delta \quad \Gamma, \beta \rightarrow \alpha, \Delta}{\Gamma, (\alpha \oplus \beta) \rightarrow \Delta} \qquad\qquad \textbf{right}\ \frac{\Gamma, \alpha, \beta \rightarrow \Delta \quad \Gamma \rightarrow \alpha, \beta, \Delta}{\Gamma \rightarrow (\alpha \oplus \beta), \Delta}$$

Here Γ and Δ are finite sequences of zero or more formulas. Each rule allows the sequent under the line to be derived from the sequent(s) above the line.

A PK(2) proof of a sequent $\Gamma \rightarrow \Delta$ is a finite sequence of sequents ending in $\Gamma \rightarrow \Delta$, such that each sequent is either an axiom or follows from earlier sequents by a rule.

Note that if π is a PK(2) proof, α is a formula, and p is a propositional variable, then the result of substituting α for p throughout π is again a PK(2) proof.

A sequent $\Gamma \rightarrow \Delta$ is *valid* iff the conjunction of the formulas in Γ implies the disjunction of the formulas in Δ. The system PK(2) is sound and complete; that is, a sequent has a PK(2)-proof iff it is valid. Soundness follows from the facts that axioms are valid, and the rules preserve validity. For completeness, that every valid sequent $\Gamma \rightarrow \Delta$ has a (Cut-free) PK(2)-proof is proved by induction on the total number of connectives in Γ and Δ, using the facts that for each introduction rule, (i) the number of connectives in the sequent below the line is more than the number of connectives in each sequent above the line, and (ii) if the sequent below the line is valid, then each sequent above the line is valid.

The *depth* of a PK(2) formula is defined by thinking of the connectives $\wedge, \vee$, and $\oplus$ as having unlimited fanin. If we think of a formula as a binary tree, then the depth of each branch is defined by counting any consecutive run of any of these connectives as a single connective. In particular, if $p_1, \ldots, p_n$ are atoms, then the formula $(p_1 \oplus \ldots \oplus p_n)$ has depth one, no matter how parentheses are inserted to make it a proper formula (with $\oplus$ a binary operator).

The depth of a sequent is the maximum of the depths of the formulas in the sequent.

The systems $\mathrm{PK}_{BD}(2)$ are bounded-depth restrictions of PK(2). For each $d \geq 1$ the system $\mathrm{PK}_{BD[d]}(2)$ is the restriction of PK(2) obtained by requiring that each formula in a proof has depth at most d. We refer to the systems $\mathrm{PK}_{BD[d]}(2)$ collectively as $\mathrm{PK}_{BD}(2)$. The systems $\mathrm{PK}_{BD}(2)$ are p-equivalent to the systems $\mathbf{AC}^0(2)$ in the sequence (57).

If Γ is a finite sequence $\alpha_1, \ldots, \alpha_n$ of formulas, then $\bigwedge \Gamma = (\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_n)$ is the conjunction of the formulas, with parentheses inserted (say, with association to the right). Similarly for $\bigvee \Gamma$ and $\bigoplus \Gamma$. For the case that Γ is empty, we define $\bigwedge \varnothing = \mathtt{T}$, $\bigvee \varnothing = \mathtt{F}$, and $\bigoplus \varnothing = \mathtt{F}$.

In describing $\mathrm{PK}_{BD}(2)$ proofs it does not much matter how parentheses are inserted in the formulas $\bigwedge \Gamma$, $\bigvee \Gamma$, and $\bigoplus \Gamma$. This is because the associative laws are valid, so that for example the sequent $\alpha \oplus (\beta \oplus \gamma) \rightarrow (\alpha \oplus \beta) \oplus \gamma$ is valid and has a Cut-free PK(2) proof with a constant number of sequents whose depths are bounded by the depth of the conclusion. From this it is easy to see that if A and A' are formulas resulting from inserting parentheses in $(\alpha_1 \oplus \ldots \oplus \alpha_n)$ in different ways, then the sequent $A \rightarrow A'$ has a PK(2) proof (using the Cut rule) with $O(n)$ sequents whose depths are bounded by the depth of the conclusion. Similarly for $\wedge$ and $\vee$.

6.3 Translations of LA over $\mathbb{Z}_2$

Suppose that the underlying field for LA is $\mathbb{Z}_2$. Let α be a formula of LA, and let σ be an object assignment which assigns a natural number $\sigma(i)$ to each free index variable i in α, and assigns natural numbers $\sigma(\mathtt{r}(A)), \sigma(\mathtt{c}(A))$ to each of the terms $\mathtt{r}(A), \mathtt{c}(A)$ respectively, where A is any matrix variable in α. Let $|\sigma|$ be the largest value assigned by σ. To each variable of type field in α we assign a propositional variable asserting that the field variable is 1 (as opposed to 0). To each matrix variable A we assign enough propositional variables to determine all entries in A (where the size of A is determined by σ). Now α and σ translate into a propositional formula $\|\alpha\|_\sigma$ of size polynomial in $|\sigma|$ which is valid iff α is valid in the standard model under σ over the field $\mathbb{Z}_2$. The method of translation is similar to those described in Chapter 9 of [Kra95].

As an example, let α be the formula $A+B = B+A$, and let σ determine that A and B are 3×3, so $\sigma(\mathtt{r}(A)) = \sigma(\mathtt{c}(A)) = \sigma(\mathtt{r}(B)) = \sigma(\mathtt{c}(B)) = 3$. Then the propositional formula $\|\alpha\|_\sigma$ involves the propositional variables $A_{pq}, B_{pq}, 1 \le p, q \le 3$ expressing the entries of A and B. In fact $\|\alpha\|_\sigma$ is

$$\bigwedge_{\substack{1\le p\le 3\\ 1\le q\le 3}} ((A_{pq} \oplus B_{pq}) \leftrightarrow (B_{pq} \oplus A_{pq}))$$

We now describe the translation in more detail. Each term m of type index is translated into a natural number $\|m\|_\sigma \in \mathbb{N}$ using σ and the intended interpretations of the function and predicate symbols (2). This is possible because the value of every index term is independent of the field values given field variables and the field entries of matrix variables. In particular, an index term of the form $\mathrm{cond}(\alpha, t_1, t_2)$ can be evaluated explicitly because of our stated restriction that all atomic subformulas of α must have the form $m_1 \le m_2$ or $m_1 = m_2$, and these formulas can be evaluated explicitly.

Each term t of type field is translated into a propositional formula $\|t\|_\sigma$ whose variables are those associated with the field variables in t, and the variables A_{pq} associated with the matrix variables A in t, where $1 \le p \le \sigma(\mathtt{r}(A))$ and $1 \le q \le \sigma(\mathtt{c}(A))$. Here $\|t\|_\sigma$ is defined by structural induction on t. The base cases are $\|0_{\text{field}}\|_\sigma = \mathtt{F}$, $\|1_{\text{field}}\|_\sigma = \mathtt{T}$, $\|a\|_\sigma = a$, and

$$\|\mathtt{e}(A, m, n)\|_\sigma = \begin{cases} A_{\|m\|_\sigma \|n\|_\sigma} & \text{if } 1 \le \|m\|_\sigma \le \sigma(\mathtt{r}(A)) \text{ and } 1 \le \|n\|_\sigma \le \sigma(\mathtt{c}(A)) \\ \mathtt{F} & \text{otherwise} \end{cases}$$

The inductive cases are as follows. First the field operations are handled by $\|t +_{\text{field}} u\|_\sigma = (\|t\|_\sigma \oplus \|u\|_\sigma)$, $\|t *_{\text{field}} u\|_\sigma = (\|t\|_\sigma \wedge \|u\|_\sigma)$, $\|-t\|_\sigma = \|t\|_\sigma$, and $\|t^{-1}\|_\sigma = \|t\|_\sigma$. The conditional is handled by

$$\|\mathrm{cond}(\beta, t, u)\|_\sigma = \begin{cases} \|t\|_\sigma & \text{if } \|\beta\|_\sigma = \mathtt{T} \\ \|u\|_\sigma & \text{otherwise} \end{cases}$$

where $\|\beta\|_\sigma$ is either $\mathtt{T}$ or $\mathtt{F}$ because of our syntactic restriction on the atomic subformulas of β.

The constructed terms are handled by

$$\|\mathtt{e}(\lambda ij\langle m', n', t\rangle, m, n)\|_\sigma = \begin{cases} \|t\|_{\sigma'} & \text{if } 1 \le \|m\|_\sigma \le \|m'\|_\sigma \text{ and } 1 \le \|n\|_\sigma \le \|n'\|_\sigma \\ \mathtt{F} & \text{otherwise} \end{cases}$$

where σ' is the same as σ except $\sigma'(i) = \|m\|_\sigma$ and $\sigma'(j) = \|n\|_\sigma$.

Finally, we deal with $\Sigma(T)$ as follows:

$$\|\Sigma(A)\|_\sigma = \bigoplus(A_{11}, A_{12}, \ldots, A_{\sigma(\mathtt{r}(A))\sigma(\mathtt{c}(A))})$$

$$\|\Sigma(\lambda ij\langle m, n, t\rangle)\|_\sigma = \bigoplus(\{\|t\|_{\sigma_{pq}}\}_{\substack{1\le p\le \|m\|_\sigma\\ 1\le q\le \|n\|_\sigma}})$$

where σ_{pq} is the same as σ except $\sigma_{pq}(i) = p$ and $\sigma_{pq}(j) = q$.

This completes the definition of $\|t\|_\sigma$ for terms t of type field. Note that the only cases for which $\oplus$ is really necessary to achieve a bounded depth polynomial size translation are those involving Σ terms.

It remains to define the translation $\|\alpha\|_\sigma$ of a formula α. If m and n are terms of type index, then the atomic formulas $m \leq n$ and $m = n$ are translated to either $\mathtt{T}$ or $\mathtt{F}$, using the natural number values of $\|m\|_\sigma$ and $\|n\|_\sigma$. If t and u are terms of type field, then $t = u$ is translated to the propositional formula $(\|t\|_\sigma \leftrightarrow \|u\|_\sigma)$.

If T and U are terms of type matrix, the the case $\|T = U\|_\sigma$ is more complicated. If T and U do not have compatible sizes, that is, if $\|\mathtt{r}(T)\|_\sigma \neq \|\mathtt{r}(U)\|_\sigma$ or $\|\mathtt{c}(T)\|_\sigma \neq \|\mathtt{c}(U)\|_\sigma$, then $\|T = U\|_\sigma = \mathtt{F}$. Suppose now that T and U have compatible sizes, and let r, c be defined as follows:

$$
\begin{aligned}
r &:= \|\mathtt{r}(T)\|_\sigma = \|\mathtt{r}(U)\|_\sigma \\
c &:= \|\mathtt{c}(T)\|_\sigma = \|\mathtt{c}(U)\|_\sigma
\end{aligned}
$$

Assume that i, j are index variables that do not occur free in T or U. Then:

$$
\|T = U\|_\sigma = \bigwedge_{1 \leq p \leq r, 1 \leq q \leq c} (\|\mathtt{e}(T, i, j)\|_{\sigma_{pq}} \leftrightarrow \|\mathtt{e}(U, i, j)\|_{\sigma_{pq}})
$$

where (as before) σ_{pq} is the same as σ except $\sigma_{pq}(i) = p$ and $\sigma_{pq}(j) = q$.

This completes the definitions of $\|\alpha\|_\sigma$ when α is an atomic formula. In general, formulas of LA are built from atomic formulas using the connectives $\wedge, \vee, \neg$. We define $\|\alpha \wedge \beta\|_\sigma, \|\alpha \vee \beta\|_\sigma, \|\neg\alpha\|_\sigma$ respectively by $\|\alpha\|_\sigma \wedge \|\beta\|_\sigma$, $\|\alpha\|_\sigma \vee \|\beta\|_\sigma$, and $\neg\|\alpha\|_\sigma$.

Theorem 6.1 For every formula α of LA there exists a polynomial p_α and a constant d_α such that for every object assignment σ to α, the length of $\|\alpha\|_\sigma$ is bounded by $p_\alpha(|\sigma|)$ and the depth of α is bounded by d_α. Further, α is valid under σ in the standard model over the field $\mathbb{Z}_2$ iff $\|\alpha\|_\sigma$ is a tautology.

Proof. The length and depth bounds are proved by structural induction on α, while simultaneously proving polynomial bounds $p_m(|\sigma|)$ on the numerical value $\|m\|_\sigma$, for each index term m, and $p_t(|\sigma|)$ on the length of the formula $\|t\|_\sigma$ for each field term t (as well as depth bounds on $\|t\|_\sigma$). The validity claim is also proved by structural induction on α, while simultaneously noting that $\|m\|_\sigma$ and $\|t\|_\sigma$ correctly evaluate index and field terms. □

Any theorem of LA is valid in the standard model for any object assignment σ over any field, including $\mathbb{Z}_2$. Thus if α is a theorem of LA, then by Theorem 6.1 the family $\langle \|\alpha\|_\sigma :$ σ is an object assignment$\rangle$ is a family of tautologies of size bounded by a polynomial in $|\sigma|$. The next theorem states that this family has polynomial size $\mathrm{PK}_{BD}(2)$-proofs.

Theorem 6.2 For every theorem α of LA there exists a polynomial q_α and a constant d_α such that for every object assignment σ to the variables of α there exists a PK(2) proof of $\|\alpha\|_\sigma$ of size at most $q_\alpha(|\sigma|)$ and depth at most d_α.

The proof is by induction on the number of sequents in the LA proof of α. See [Sol01] for details.

It is tempting to conjecture that the translations of the matrix identity (55) into a family of PK(2) formulas do not have polynomial size bounded depth PK(2) proofs. By Theorem 6.2 this would imply that (55) is not a theorem of LA. Unfortunately, as mentioned before, it is an open question even whether $\mathrm{PK}_{BD}(2)$ is a polynomially bounded proof system.

6.4 Translations of LA over $\mathbb{Z}_p$

If the characteristic of the underlying field is $p > 2$, then the corresponding propositional proof system should have connectives that count mod p. This can be done by introducing a propositional connective $\mathtt{MOD}_{p,i}$ of unbounded arity for each i such that $0 \le i < p$. More generally, for every pair a, i with $a \ge 2$ and $0 \le i < a$ we introduce a connective $\mathtt{MOD}_{a,i}$ of unbounded arity (see [Kra95, Chapter 12.6]) defined by the condition that if $k \ge 0$ and $\Gamma = \alpha_1, ..., \alpha_k$ is a finite sequence of formulas, then

$$\mathtt{MOD}_{a,i}(\Gamma) \text{ is true} \quad \text{iff} \quad |\{j : \alpha_j \text{ is true}\}| \pmod a = i$$

For $a \ge 2$, the propositional proof system PK(a) allows formulas built from the connectives $\mathtt{MOD}_{a,i}$ for $0 \le i < a$ in addition to the usual connectives of PK. In addition to the axiom schemes and rules of PK, the system PK(a) allows the axioms

$\to \mathtt{MOD}_{a,0}(\varnothing)$
$\to \neg\mathtt{MOD}_{a,i}(\varnothing)$, for $1 \le i < a$
$\to (\mathtt{MOD}_{a,i}(\Gamma, \alpha) \leftrightarrow [\mathtt{MOD}_{a,i}(\Gamma) \wedge \neg\alpha) \vee (\mathtt{MOD}_{a,i-1}(\Gamma) \wedge \alpha)])$, for $0 \le i < a$, where $i-1$ is taken mod a

We denote the bounded depth versions of PK(p) by PK$_{BD}(p)$.

For $a = 2$ it is not hard to see that the systems PK(2) and PK$_{BD}(2)$ just defined are equivalent to the systems PK(2) and PK$_{BD}(2)$ defined in section 6.2 using the $\oplus$ connective. A formula $\mathtt{MOD}_{2,1}(\Gamma)$ can be translated to $\bigoplus(\Gamma)$, and $\mathtt{MOD}_{2,0}(\Gamma)$ can be translated to $\neg\bigoplus(\Gamma)$.

When the underlying field is $\mathbb{Z}_p$, for p a prime, formulas of LA translate into families of propositional formulas of PK$_{BD}(p)$. The translation is similar to that described in section 6.3 for $p = 2$. The main difference for $p > 2$ is that now field elements must be encoded by a string of propositional variables instead of a single propositional variable.

The element i in $\mathbb{Z}_p = \{0, 1, ..., p-1\}$ is represented by the string $\mathtt{T}^i\mathtt{F}^{p-1-i}$. For example, the elements $0, 1, 2, 3, 4$ of $\mathbb{Z}_5$ are represented by $\mathtt{FFFF}, \mathtt{TFFF}, \mathtt{TTFF}, \mathtt{TTTF}, \mathtt{TTTT}$, respectively. Each term t of type field translates into $p-1$ propositional formulas $\|t\|^1_\sigma, ..., \|t\|^{p-1}_\sigma$ for the $p-1$ bits representing the value of t. (Properly we should use the notation $\|t\|^j_{\sigma,p}$ to indicate the dependence of the formula on p. However we mostly omit p to avoid subscript clutter.) These formulas are defined by structural induction on t, as for the case $p = 2$. The propositional variables in $\|t\|^j_\sigma$ consist of a tuple $a_1, ..., a_{p-1}$ for each field variable a in t, and an array of variables A^k_{ij} for each matrix variable A in t.

For convenience, we define $\|t\|^j_\sigma = \mathtt{F}$, for $j \ge p$.

The base cases are given by
$\|0_{\text{field}}\|^j_\sigma = \mathtt{F}, 1 \le j < p$
$\|1_{\text{field}}\|^1_\sigma = \mathtt{T}, \qquad \|1_{\text{field}}\|^j_\sigma = \mathtt{F}, 2 \le j < p$
$\|a\|^j_\sigma = a_j, 1 \le j < p$
$\|e(A, m, n)\|^k_\sigma = A^k_{\|m\|_\sigma \|n\|_\sigma}$ (or $\mathtt{F}$), $1 \le k < p$

The induction step is given by

$$\begin{aligned}
\|t+u\|_\sigma^j &= \bigvee_{j\le i<p} \mathtt{MOD}_{p,i}(\{\|t\|_\sigma^k\}_{1\le k<p}, \{\|u\|_\sigma^k\}_{1\le k<p}) \\
\|t*u\|_\sigma^j &= \bigvee_{\substack{1\le i,k<p \\ j\le (ik \bmod p)}} (\|t\|_\sigma^i \wedge \neg\|t\|_\sigma^{i+1}) \wedge (\|u\|_\sigma^k \wedge \neg\|u\|_\sigma^{k+1}) \\
\|-t\|_\sigma^j &= \bigvee_{\substack{1\le i<p \\ j\le p-i}} (\|t\|_\sigma^i \wedge \neg\|t\|_\sigma^{i+1}) \\
\|t^{-1}\|_\sigma^j &= \bigvee_{\substack{1\le i,k<p \\ j\le k\wedge ik\equiv 1 \bmod p}} (\|t\|_\sigma^i \wedge \neg\|t\|_\sigma^{i+1}) \\
\|\Sigma(A)\|_\sigma^j &= \bigvee_{j\le i<p} \mathtt{MOD}_{p,i}(\{A_{xy}^k\}_{1\le x\le\sigma(\mathtt{r}(A)),1\le y\le\sigma(\mathtt{c}(A)),1\le k<p})
\end{aligned}$$

(We omit the cases $\|\mathrm{cond}(\beta,t,u)\|_\sigma^j$, $\|\mathtt{e}(\lambda ij\langle m',n',t\rangle,m,n)\|_\sigma^k$ and $\|\Sigma(\lambda ij\langle m,n,t\rangle)\|_\sigma^k$.)

Now formulas α of LA are translated to formulas $\|\alpha\|_{\sigma,p}$ as in section 6.3 except that if t,u are terms of type field, then

$$\|t=u\|_{\sigma,p} = \bigwedge_{1\le j<p} (\|t\|_{\sigma,p}^j \leftrightarrow \|u\|_{\sigma,p}^j)$$

and similarly for $\|T=U\|_{\sigma,p}$ for terms T,U of type matrix.

Finally, in order to ensure that the string $a_1\ldots a_{p-1}$ of propositional variables properly codes a value in $\mathbb{Z}_p$ for the field variable a we need the assumptions

$$a_{i+1}\supset a_i, \qquad 1\le i<p-1 \tag{58}$$

and similarly for each matrix variable A we need the assumptions

$$A_{ij}^{k+1}\supset A_{ij}^k, \qquad 1\le i\le\sigma(\mathtt{r}(A)), 1\le j\le\sigma(\mathtt{c}(A)), 1\le k<p-1 \tag{59}$$

Let $\Gamma_{\alpha,p}$ be the sequence of all such assumption formulas for all field variables a in α and all matrix variables A in α. Then the analogs of Theorems 6.1 and 6.2 hold over the field $\mathbb{Z}_p$ where we replace $\|\alpha\|_\sigma$ by the sequent $\Gamma_{\alpha,p}\to\|\alpha\|_{\sigma,p}$ and PK(2) by PK(p).

6.5 Translation of LA over arbitrary finite fields and $\mathbb{Q}$

Every finite field K of characteristic p is a d-dimensional vector space over $\mathbb{Z}_p$ for some $d\ge 1$ in $\mathbb{N}$. Hence each element of K is naturally represented by a d-tuple of elements of $\mathbb{Z}_p$, where addition is defined componentwise. Therefore the translation of LA formulas α to propositional formulas $\|\alpha\|_{\sigma,p}$ of PK(p) giving the meaning of α over the field $\mathbb{Z}_p$ easily extends to a translation $\|\alpha\|_{\sigma,K}$ (also a PK(p) formula) giving the meaning of α over the field K. The analogs of the assumptions (58) and (59) for all field and matrix variables in a formula α over the field K are expressed by the sequence $\Gamma_{\alpha,K}$.

An element $r\in\mathbb{Q}$ can be represented by a pair of integers $(x,y), y\ne 0$, where $r=x/y$ and each of x,y is represented in binary notation. Using this notation, all of the field operations $+,-,*,^{-1}$ can be carried out in the complexity class $\mathbf{TC}^0$ (56), as well as the computation $\Sigma(A)$ for a rational matrix A. Thus each LA formula α translates into a family $\langle\|\alpha\|_{\sigma,\mathbb{Q}}\rangle$ of $\mathbf{TC}^0$ formulas of size polynomial in $|\sigma|$, expressing the meaning of α under σ over $\mathbb{Q}$. The analogs of assumptions (58) and (59) when $K = \mathbb{Q}$ simply assert that $y \neq 0$ in the pair (x, y). Let $\Gamma_{\alpha,\mathbb{Q}}$ be the sequence of all such assumption formulas for field and matrix variables occurring in α.

The corresponding propositional proof system is $\mathbf{TC}^0$-Frege (57). Many properties of integer arithmetic have been formalized as efficient $\mathbf{TC}^0$-Frege proofs in [BPR00]. From this it is clear that if α is a theorem of LA, then the family $\langle \Gamma_{\alpha,\mathbb{Q}} \to \|\alpha\|_{\sigma,\mathbb{Q}} \rangle$ has polynomial size $\mathbf{TC}^0$-Frege proofs.

Now Theorems 6.1 and 6.2 can be generalized as follows.

Theorem 6.3 Let K be either a finite field of characteristic p, or let $K = \mathbb{Q}$. Let $S(K)$ be the collection of propositional proof systems $\mathrm{PK}_{BD}(p)$ if K is finite, or $\mathbf{TC}^0$-Frege if $K = \mathbb{Q}$. Let α be a formula of LA. Then

$$\langle \Gamma_{\alpha,K} \to \|\alpha\|_{\sigma,K} : \ \sigma \text{ is an object assignment} \rangle \tag{60}$$

is a family of propositional sequents in the notation of $S(K)$ of size polynomial in $|\sigma|$ such that $\Gamma_{\alpha,K} \to \|\alpha\|_{\sigma,K}$ is valid iff α is valid under σ in the standard model over K. Further, if α is a theorem of LA, then (60) has polynomial size proofs in one of the $S(K)$ systems.

6.6 Translations of LAP and ∀LAP

Matrix powering can be efficiently computed using the recursion

$$A^0 = I \tag{61}$$

$$A^m = \begin{cases} (A^{m \texttt{ div } 2})^2 & \text{if } m \text{ is even} \\ (A^{m \texttt{ div } 2})^2 * A & \text{otherwise} \end{cases} \tag{62}$$

If the underlying field K is finite or $\mathbb{Q}$, and (in the case of $\mathbb{Q}$) the entries of A are represented by strings of length $O(n)$, then using the notation for field elements discussed above, for an $n \times n$ matrix A, each bit of each entry of A^m, $m \leq n$, can be expressed using this recursion by a propositional formula of size $2^{O(\log^2 n)}$ ("quasi-polynomial size"). It is well-known that this recursion also places matrix powering in the complexity class $\mathbf{NC}^2$.

Since the language of LAP is obtained from that for LA by adding matrix terms of the form $\mathtt{P}(m, T)$, this tells us how to extend the translations of LA formulas to obtain propositional translations $\Gamma_{\alpha,K} \to \|\alpha\|_{\sigma,K}$ of a LAP formula α of quasi-polynomial size in $|\sigma|$.

Now we claim that if α is a theorem of LAP, then the translations have quasi-polynomial size PK proofs (and hence quasi-polynomial size Frege proofs). The extra work (over the proof of Theorem 6.3) in proving this is showing that the translations of the two new axioms

A35 $\to \mathtt{P}(0, A) = I$
A36 $\to \mathtt{P}(m + 1, A) = \mathtt{P}(m, A) * A$.

have quasi-polynomial size PK proofs. This is not immediate, because the recursion (61,62) used to construct the formulas translating $\mathtt{P}(m, A)$ is not the same as the recursion expressed by these axioms. However, it can be shown by induction on $\log_2 m$ that the translations of both **A36** and the equation $\mathtt{P}(m+1, A) = A * \mathtt{P}(m, A)$ have PK proofs of size $2^{O((\log m)(\log n))}$, for an $n \times n$ matrix A with entries of size $O(n)$. Here we use the fact that LA proves the associative law $A(BC) = (AB)C$ (**T13**), so by Theorem 6.3 the translation of (**T13**) has polynomial size Frege proofs.

It is an open questions whether the translations (over any field) of the hard matrix identities such as (55) have quasi-polynomial size Frege proofs. This would follow if LAP proves these identities.

Presumably if α is a theorem of LAP, then suitable propositional translations can be defined which have polynomial size $\mathbf{NC}^2$-Frege proofs, but we have not worked this out in detail.

The theory $\forall$LAP can be interpreted in the second order theory $\mathbf{V}_1^1$ of bounded arithmetic. The latter is isomorphic to Buss's first order theory S_2^1 [Bus86], one of the standard theories formalizing polynomial time (feasible) reasoning. The images of the quantifier-free theorems of $\forall$LAP in $\mathbf{V}_1^1$ (or in S_2^1) translate into tautology families with polynomial size eFrege (Extended Frege) proofs (see (57)). Thus by the results in section 5, the propositional translations of the hard matrix identities and the Cayley-Hamilton theorem have polynomial size eFrege proofs.

The theories $\mathbf{V}_1^1$ and S_2^1, and their propositional translations, are treated extensively in [Kra95].

7 Conclusion and Open Problems

A major result in this paper is a (perhaps the first) feasible proof of the Cayley-Hamilton theorem. This is the contents of Theorem 5.1, which states that the theory $\forall$LAP proves the C-H theorem. Intuitively, proofs in $\forall$LAP are restricted to polynomial time concepts, as evidenced by the translations of $\forall$LAP into the theories $\mathbf{V}_1^1$ and S_2^1 discussed in section 6.

We also show that most basic results in linear algebra, including hard matrix identities such as $AB = I \rightarrow BA = I$, have feasible proofs (proofs in $\forall$LAP).

On the other hand we formalize Berkowitz's algorithm in the weaker theory LAP, but we leave open whether that theory proves the C-H theorem. Since the most complex operation in LAP is matrix powering, and since matrix powering (over finite fields and $\mathbb{Q}$) is in the complexity class NC^2, this question can be restated to ask whether C-H can be proved using only concepts in NC^2. We also leave open whether the hard matrix identities have such proofs.

The hard matrix identities have natural translations into families of propositional tautologies. Since the identities can be proved in the theory $\forall$LAP, it follows by a general result that their propositional translations have polynomial size eFrege proofs. If LAP could prove the C-H theorem, then the results of section 4 show that LAP proves the hard matrix identities, and hence by the results in section 6 the translated identities would have quasi-polynomial size Frege proofs. At present it is open whether these tautologies have sub-exponential size Frege proofs.

Here are some other open questions. More details can be found in Chapter 9 of [Sol01].

1. Show that LA cannot prove $AB = I \rightarrow BA = I$. The most obvious approach is to construct a model $\mathcal{M}$ of LA such that $\mathcal{M} \not\models AB = I \rightarrow BA = I$. An alternative approach is given in [SU03] where it is shown that if LA $\vdash AB = I \rightarrow BA = I$, then the Propositional Pigeonhole Principal has polynomial size bounded-depth Frege proofs with mod 2 gates. The latter is believed to be unlikely.

2. Is $AB = I \rightarrow BA = I$ "Complete"? Theorem 4.1 states that LAP proves that the C-H theorem implies $AB = I \rightarrow BA = I$. Could it be that LAP+ C-H is a conservative extension of LA + $AB = I \rightarrow BA = I$?

3. Does LAP prove $\det(A) = 0 \rightarrow AB \neq I$? If so, then LAP proves the equivalence of the multiplicativity of the determinant with the other three principles of section 4.

Acknowledgments: Our thanks to Sam Buss for fruitful comments resulting from the careful reading of the source of this paper: the first author's PhD thesis [Sol01].

References

[Ajt88] M. Ajtai. The complexity of the pigeonhole principle. In *Proceedings of the IEEE 29th Annual Symposium on Foundations of Computer Science*, pages 346–355, 1988.

[Ara00] Noriko H. Arai. Tractability of cut-free Gentzen type propositional calculus with permutation inference. *Theoretical Computer Science*, 243:185–197, 2000.

[BBP94] M. Bonet, S. Buss, and T. Pitassi. Are there hard examples for Frege systems? *Feasible Mathematics*, II:30–56, 1994.

[Ber84] Stuart J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, 18(3):147–150, 1984.

[BPR00] M. L. Bonet, T. Pitassi, and R. Raz. On interpolation and automatization for frege systems. *SIAM J. on Computing*, 29:1939–1967, 2000.

[Bus86] Samuel R. Buss. *Bounded Arithmetic*. Studies in proof theory. Napoli, 1986.

[Bus87] Samuel R. Buss. The propositional pigionhole principle has polynomial size frege proofs. *J. Symbolic Logic*, 52:916–927, 1987.

[Bus98] Samuel R. Buss. An introduction to proof theory. In Samuel R. Buss, editor, *Handbook of Proof Theory*, pages 1–78. North Holland, 1998.

[Coo75] Stephen A. Cook. Feasibly constructive proofs and the propositional calculus. *Proc. 7th ACM Symposium on the Theory of Computation*, pages 83–97, 1975.

[Coo85] Stephen A. Cook. A taxonomy of problems with fast parallel algorithms. *Information and Computation*, 64(13):2–22, 1985.

[Kra95] Jan Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory*. Cambridge, 1995.

[SC02] Michael Soltys and Stephen Cook. The proof complexity of linear algebra. In *Seventeenth Annual IEEE Symposium on Logic in Computer Science*, pages 335–344, 2002.

[Sol01] Michael Soltys. *The Complexity of Derivations of Matrix Identities*. PhD thesis, University of Toronto, Department of Mathematics, 2001. Available from the Electronic Colloquium on Computational Complexity (`http://www.eccc.uni-trier.de/eccc/`).

[Sol02] Michael Soltys. Extended Frege and Gaussian Elimination. *Bulletin of the Section of Logic*, 31(4):1–17, 2002.

[SU03] Michael Soltys and Alasdair Urquhart. Matrix identities and the Pigeonhole Principle. *Archive for Mathematical Logic*, 2003. To appear.

[Urq95] Alasdair Urquhart. The complexity of propositional proofs. *Bulletin of Symbolic Logic*, 1(4):425–467, 1995.

[Urq98] Alasdair Urquhart. The symmetry rule in propositional logic. *Discrete Applied Mathematics*, 96–97:177–193, 1998.

[vzG93] Joachim von zur Gathen. Parallel linear algebra. In John H. Reif, editor, *Synthesis of Parallel Algorithms*, pages 574–617. Morgan and Kaufman, 1993.